NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **HIPAA Simplification 2013 (Security & Privacy)**
Focal Document URL: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-law-hipaa-simplification-2013.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.102	Statutory basis	[see focal document for details]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.103	Definitions	[see focal document for details]	Functional	Subset Of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
§ 164.104	Applicability	[see focal document for details]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.105	Organizational requirements	[see focal document for details]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.106	Relationship to other parts	In complying with the requirements of this part, covered entities and, where provided, business associates, are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.302	Applicability	[see focal document for details]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.304	Definitions	[see focal document for details]	Functional	Subset Of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
§ 164.306	Security standards: General rules	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.306(a)	General requirements	Covered entities and business associates must do the following:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.306(a)(1)	N/A	Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
§ 164.306(a)(1)	N/A	Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	Functional	Subset Of	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
§ 164.306(a)(1)	N/A	Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	Functional	Subset Of	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
§ 164.306(a)(1)	N/A	Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	Functional	Subset Of	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
§ 164.306(a)(1)	N/A	Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	Functional	Subset Of	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:(1) Implemented correctly; and(2) Operating as intended.	10	
§ 164.306(a)(1)	N/A	Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	Functional	Subset Of	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	10	
§ 164.306(a)(1)	N/A	Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.	Functional	Subset Of	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.	10	
§ 164.306(a)(2)	N/A	Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
§ 164.306(a)(3)	N/A	Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
§ 164.306(a)(3)	N/A	Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
§ 164.306(a)(3)	N/A	Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
§ 164.306(b)	Flexibility of approach	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.306(b)(1)	N/A	Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.	Functional	Intersects With	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal security, compliance and resilience control system.	5	
§ 164.306(b)(1)	N/A	Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.	Functional	Subset Of	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
§ 164.306(b)(1)	N/A	Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
§ 164.306(b)(1)	N/A	Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	
§ 164.306(b)(1)	N/A	Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	3	
§ 164.306(b)(2)	N/A	In deciding which security measures to use, a covered entity or business associate must take into account the following factors:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.306(b)(2)(i)	N/A	The size, complexity, and capabilities of the covered entity or business associate.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
§ 164.306(b)(2)(i)	N/A	The size, complexity, and capabilities of the covered entity or business associate.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines:(1) The resulting risk to organizational operations, assets, individuals and other organizations; and(2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
§ 164.306(b)(2)(ii)	N/A	The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
§ 164.306(b)(2)(ii)	N/A	The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	
§ 164.306(b)(2)(iii)	N/A	The costs of security measures.	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
§ 164.306(b)(2)(iv)	N/A	The probability and criticality of potential risks to electronic protected health information.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
§ 164.306(b)(2)(iv)	N/A	The probability and criticality of potential risks to electronic protected health information.	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify:(1) Assumptions affecting risk assessments, risk response and risk monitoring;(2) Constraints affecting risk assessments, risk response and risk monitoring;(3) The organizational risk tolerance; and(4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
§ 164.306(b)(2)(iv)	N/A	The probability and criticality of potential risks to electronic protected health information.	Functional	Intersects With	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that:(1) Document the security categorization results (including supporting rationale) in the security plan for systems; and(2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	
§ 164.306(b)(2)(iv)	N/A	The probability and criticality of potential risks to electronic protected health information.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
§ 164.306(b)(2)(iv)	N/A	The probability and criticality of potential risks to electronic protected health information.	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
§ 164.306(b)(2)(iv)	N/A	The probability and criticality of potential risks to electronic protected health information.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
§ 164.306(b)(2)(iv)	N/A	The probability and criticality of potential risks to electronic protected health information.	Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
§ 164.306(b)(2)(iv)	N/A	The probability and criticality of potential risks to electronic protected health information.	Functional	Intersects With	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5	
§ 164.306(c)	Standards	A covered entity or business associate must comply with the applicable standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
§ 164.306(d)	Implementation specifications	In this subpart:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.306(d)(1)	N/A	Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
§ 164.306(d)(2)	N/A	When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
§ 164.306(d)(3)	N/A	When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must—	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.306(d)(3)(i)	N/A	Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
§ 164.306(d)(3)(i)	N/A	Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.306(d)(3)(i)	N/A	Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
§ 164.306(d)(3)(ii)	N/A	As applicable to the covered entity or business associate—	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.306(d)(3)(ii)(A)	N/A	Implement the implementation specification if reasonable and appropriate; or	Functional	Subset Of	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
§ 164.306(d)(3)(ii)(B)	N/A	If implementing the implementation specification is not reasonable and appropriate—	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.306(d)(3)(ii)(B)(1)	N/A	Document why it would not be reasonable and appropriate to implement the implementation specification; and	Functional	Subset Of	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	10	
§ 164.306(d)(3)(ii)(B)(2)	N/A	Implement an equivalent alternative measure if reasonable and appropriate.	Functional	Equal	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	10	
§ 164.306(e)	Maintenance	A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with § 164.316(b)(2)(iii).	Functional	Equal	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	10	
§ 164.308	Administrative safeguards	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)	N/A	A covered entity or business associate must, in accordance with § 164.306:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)(1)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)(1)(i)	Standard: Security management process	Implement policies and procedures to prevent, detect, contain, and correct security violations.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.308(a)(1)(i)	Standard: Security management process	Implement policies and procedures to prevent, detect, contain, and correct security violations.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
§ 164.308(a)(1)(i)	Standard: Security management process	Implement policies and procedures to prevent, detect, contain, and correct security violations.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
§ 164.308(a)(1)(i)	Standard: Security management process	Implement policies and procedures to prevent, detect, contain, and correct security violations.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
§ 164.308(a)(1)(i)	Standard: Security management process	Implement policies and procedures to prevent, detect, contain, and correct security violations.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
§ 164.308(a)(1)(ii)	Implementation specifications:	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)(1)(ii)(A)	Risk analysis (Required)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	Functional	Equal	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.308(a)(1)(ii)(B)	Risk management (Required)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Functional	Intersects With	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal security, compliance and resilience control system.	5	
§ 164.308(a)(1)(ii)(B)	Risk management (Required)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Functional	Subset Of	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
§ 164.308(a)(1)(ii)(C)	Sanction policy (Required)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Functional	Equal	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	10	
§ 164.308(a)(1)(ii)(D)	Information system activity review (Required)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
§ 164.308(a)(1)(ii)(D)	Information system activity review (Required)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
§ 164.308(a)(1)(ii)(D)	Information system activity review (Required)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
§ 164.308(a)(2)	Standard: Assigned security responsibility	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Functional	Equal	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	10	
§ 164.308(a)(3)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)(3)(i)	Standard: Workforce security	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.308(a)(3)(i)	Standard: Workforce security	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Functional	Intersects With	Sensitive / Regulated Data Access Enforcement	CFG-08	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated data.	5	
§ 164.308(a)(3)(i)	Standard: Workforce security	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
§ 164.308(a)(3)(i)	Standard: Workforce security	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
§ 164.308(a)(3)(i)	Standard: Workforce security	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
§ 164.308(a)(3)(ii)	Implementation specifications:	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)(3)(ii)(A)	Authorization and/or supervision (Addressable)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
§ 164.308(a)(3)(ii)(A)	Authorization and/or supervision (Addressable)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	3	
§ 164.308(a)(3)(ii)(A)	Authorization and/or supervision (Addressable)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
§ 164.308(a)(3)(ii)(A)	Authorization and/or supervision (Addressable)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5	
§ 164.308(a)(3)(ii)(B)	Workforce clearance procedure (Addressable)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
§ 164.308(a)(3)(ii)(B)	Workforce clearance procedure (Addressable)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
§ 164.308(a)(3)(ii)(B)	Workforce clearance procedure (Addressable)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
§ 164.308(a)(3)(ii)(C)	Termination procedures (Addressable)	Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Functional	Intersects With	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	5	
§ 164.308(a)(3)(ii)(C)	Termination procedures (Addressable)	Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
§ 164.308(a)(3)(ii)(C)	Termination procedures (Addressable)	Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
§ 164.308(a)(3)(ii)(C)	Termination procedures (Addressable)	Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	
§ 164.308(a)(4)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)(4)(i)	Standard: Information access management	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.308(a)(4)(i)	Standard: Information access management	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
§ 164.308(a)(4)(ii)	Implementation specifications:	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)(4)(ii)(A)	Isolating health care clearinghouse functions (Required)	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.308(a)(4)(ii)(B)	Access authorization (Addressable)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.308(a)(4)(ii)(C)	Access establishment and modification (Addressable)	Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Functional	Equal	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	10	
§ 164.308(a)(5)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)(5)(i)	Standard: Security awareness and training	Implement a security awareness and training program for all members of its workforce (including management).	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
§ 164.308(a)(5)(i)	Standard: Security awareness and training	Implement a security awareness and training program for all members of its workforce (including management).	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
§ 164.308(a)(5)(ii)	Implementation specifications:	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)(5)(ii)(A)	Security reminders (Addressable)	Periodic security updates.	Functional	Equal	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	10	
§ 164.308(a)(5)(ii)(B)	Protection from malicious software (Addressable)	Procedures for guarding against, detecting, and reporting malicious software.	Functional	Equal	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	10	
§ 164.308(a)(5)(ii)(C)	Log-in monitoring (Addressable)	Procedures for monitoring log-in attempts and reporting discrepancies.	Functional	Equal	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and(3) Annually thereafter.	10	
§ 164.308(a)(5)(ii)(D)	Password management (Addressable)	Procedures for creating, changing, and safeguarding passwords.	Functional	Equal	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and(3) Annually thereafter.	10	
§ 164.308(a)(6)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)(6)(i)	Standard: Security incident procedures	Implement policies and procedures to address security incidents.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.308(a)(6)(i)	Standard: Security incident procedures	Implement policies and procedures to address security incidents.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
§ 164.308(a)(6)(ii)	Implementation specification: Response and reporting (Required)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	Functional	Equal	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
§ 164.308(a)(7)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)(7)(i)	Standard: Contingency plan	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.308(a)(7)(i)	Standard: Contingency plan	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
§ 164.308(a)(7)(i)	Standard: Contingency plan	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
§ 164.308(a)(7)(ii)	Implementation specifications:	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(a)(7)(ii)(A)	Data backup plan (Required)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Functional	Equal	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	10	
§ 164.308(a)(7)(ii)(B)	Disaster recovery plan (Required)	Establish (and implement as needed) procedures to restore any loss of data.	Functional	Equal	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	10	
§ 164.308(a)(7)(ii)(C)	Emergency mode operation plan (Required)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
§ 164.308(a)(7)(ii)(C)	Emergency mode operation plan (Required)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	5	
§ 164.308(a)(7)(ii)(D)	Testing and revision procedures (Addressable)	Implement procedures for periodic testing and revision of contingency plans.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
§ 164.308(a)(7)(ii)(D)	Testing and revision procedures (Addressable)	Implement procedures for periodic testing and revision of contingency plans.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
§ 164.308(a)(7)(ii)(E)	Applications and data criticality analysis (Addressable)	Assess the relative criticality of specific applications and data in support of other contingency plan components.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
§ 164.308(a)(7)(ii)(E)	Applications and data criticality analysis (Addressable)	Assess the relative criticality of specific applications and data in support of other contingency plan components.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	8	
§ 164.308(a)(7)(ii)(E)	Applications and data criticality analysis (Addressable)	Assess the relative criticality of specific applications and data in support of other contingency plan components.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	
§ 164.308(a)(7)(ii)(E)	Applications and data criticality analysis (Addressable)	Assess the relative criticality of specific applications and data in support of other contingency plan components.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3	
§ 164.308(a)(8)	Standard: Evaluation	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
§ 164.308(a)(8)	Standard: Evaluation	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	5	
§ 164.308(a)(8)	Standard: Evaluation	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	3	
§ 164.308(b)	Business associate contracts and other arrangements	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.308(b)(1)	N/A	A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
§ 164.308(b)(1)	N/A	A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
§ 164.308(b)(1)	N/A	A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
§ 164.308(b)(1)	N/A	A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
§ 164.308(b)(1)	N/A	A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	
§ 164.308(b)(2)	N/A	A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.308(b)(2)	N/A	A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
§ 164.308(b)(2)	N/A	A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.	Functional	Intersects With	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration(1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to subcontractors.	5	
§ 164.308(b)(3)	Implementation specifications: Written contract or other arrangement (Required)	Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive/regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
§ 164.308(b)(3)	Implementation specifications: Written contract or other arrangement (Required)	Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	Functional	Equal	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.310	Physical safeguards	A covered entity or business associate must, in accordance with § 164.306:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.310(a)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.310(a)(1)	Standard: Facility access controls	Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.310(a)(1)	Standard: Facility access controls	Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
§ 164.310(a)(2)	Implementation specifications:	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.310(a)(2)(i)	Contingency operations (Addressable)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	Functional	Intersects With	Alternate Processing Site Accessibility	BCD-09.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate processing sites and possible mitigation actions, in the event of an area-wide disruption or disaster.	8	
§ 164.310(a)(2)(i)	Contingency operations (Addressable)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
§ 164.310(a)(2)(i)	Contingency operations (Addressable)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
§ 164.310(a)(2)(i)	Contingency operations (Addressable)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	5	
§ 164.310(a)(2)(ii)	Facility security plan (Addressable)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.310(a)(2)(ii)	Facility security plan (Addressable)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
§ 164.310(a)(2)(ii)	Facility security plan (Addressable)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
§ 164.310(a)(2)(iii)	Access control and validation procedures (Addressable)	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
§ 164.310(a)(2)(iii)	Access control and validation procedures (Addressable)	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
§ 164.310(a)(2)(iii)	Access control and validation procedures (Addressable)	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
§ 164.310(a)(2)(iii)	Access control and validation procedures (Addressable)	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
§ 164.310(a)(2)(iv)	Maintenance records (Addressable)	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.310(a)(2)(iv)	Maintenance records (Addressable)	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	Functional	Intersects With	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	8	
§ 164.310(a)(2)(iv)	Maintenance records (Addressable)	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
§ 164.310(a)(2)(iv)	Maintenance records (Addressable)	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
§ 164.310(b)	Standard: Workstation use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.310(b)	Standard: Workstation use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	
§ 164.310(b)	Standard: Workstation use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5	
§ 164.310(b)	Standard: Workstation use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	3	
§ 164.310(b)	Standard: Workstation use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	3	
§ 164.310(b)	Standard: Workstation use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
§ 164.310(b)	Standard: Workstation use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	3	
§ 164.310(b)	Standard: Workstation use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	3	
§ 164.310(b)	Standard: Workstation use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	3	
§ 164.310(c)	Standard: Workstation security	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users	Functional	Subset Of	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	10	
§ 164.310(c)	Standard: Workstation security	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
§ 164.310(c)	Standard: Workstation security	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	5	
§ 164.310(c)	Standard: Workstation security	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
§ 164.310(c)	Standard: Workstation security	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	
§ 164.310(d)	Standard: Device and media controls	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.310(d)(1)	N/A	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.310(d)(1)	N/A	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
§ 164.310(d)(1)	N/A	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Functional	Intersects With	Removal of Assets	AST-11	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	5	
§ 164.310(d)(1)	N/A	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
§ 164.310(d)(1)	N/A	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
§ 164.310(d)(1)	N/A	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	
§ 164.310(d)(1)	N/A	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	
§ 164.310(d)(1)	N/A	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
§ 164.310(d)(1)	N/A	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
§ 164.310(d)(1)	N/A	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Functional	Intersects With	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.	5	
§ 164.310(d)(2)	Implementation specifications:	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.310(d)(2)(i)	Disposal (Required)	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.310(d)(2)(i)	Disposal (Required)	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
§ 164.310(d)(2)(i)	Disposal (Required)	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
§ 164.310(d)(2)(ii)	Media re-use (Required)	Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
§ 164.310(d)(2)(ii)	Media re-use (Required)	Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
§ 164.310(d)(2)(iii)	Accountability (Addressable)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:(1) Accurately reflects the current TAASD in use;(2) Identifies authorized software products, including business justification details;(3) Is at the level of granularity deemed necessary for tracking and reporting;(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and(5) Is available for review and audit by designated organizational personnel.	3	
§ 164.310(d)(2)(iii)	Accountability (Addressable)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Functional	Intersects With	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	3	
§ 164.310(d)(2)(iii)	Accountability (Addressable)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
§ 164.310(d)(2)(iii)	Accountability (Addressable)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5	
§ 164.310(d)(2)(iii)	Accountability (Addressable)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Functional	Intersects With	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	5	
§ 164.310(d)(2)(iv)	Data backup and storage (Addressable)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3	
§ 164.312	Technical safeguards	A covered entity or business associate must, in accordance with § 164.306:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.312(a)	Standard: Access control	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.312(a)(1)	N/A	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.312(a)(1)	N/A	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
§ 164.312(a)(1)	N/A	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
§ 164.312(a)(1)	N/A	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
§ 164.312(a)(1)	N/A	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
§ 164.312(a)(1)	N/A	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
§ 164.312(a)(2)	Implementation specifications:	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.312(a)(2)(i)	Unique user identification (Required)	Assign a unique name and/or number for identifying and tracking user identity.	Functional	Subset Of	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	10	
§ 164.312(a)(2)(i)	Unique user identification (Required)	Assign a unique name and/or number for identifying and tracking user identity.	Functional	Equal	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	10	
§ 164.312(a)(2)(ii)	Emergency access procedure (Required)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Functional	Subset Of	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	10	
§ 164.312(a)(2)(ii)	Emergency access procedure (Required)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Functional	Intersects With	Removal of Temporary / Emergency Accounts	IAC-15.2	Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account.	3	
§ 164.312(a)(2)(ii)	Emergency access procedure (Required)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Functional	Equal	Emergency Accounts	IAC-15.9	Mechanisms exist to establish and control "emergency access only" accounts.	10	
§ 164.312(a)(2)(iii)	Automatic logoff (Addressable)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
§ 164.312(a)(2)(iii)	Automatic logoff (Addressable)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Functional	Intersects With	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	5	
§ 164.312(a)(2)(iv)	Encryption and decryption (Addressable)	Implement a mechanism to encrypt and decrypt electronic protected health information.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
§ 164.312(b)	Standard: Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
§ 164.312(b)	Standard: Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	
§ 164.312(b)	Standard: Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
§ 164.312(b)	Standard: Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Functional	Intersects With	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of Technology Assets, Applications and/or Services (TAAS), based on TAAS criticality and the sensitivity of the data it stores, transmits and processes.	5	
§ 164.312(b)	Standard: Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:(1) Establish what type of event occurred;(2) When (date and time) the event occurred;(3) Where the event occurred;(4) The source of the event;(5) The outcome (success or failure) of the event; and(6) The identity of any user/subject associated with the event.	5	
§ 164.312(b)	Standard: Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.312(b)	Standard: Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
§ 164.312(c)	Standard: Integrity	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.312(c)(1)	N/A	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.312(c)(1)	N/A	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
§ 164.312(c)(1)	N/A	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	5	
§ 164.312(c)(2)	Implementation specification: Mechanism to authenticate electronic protected health information (Addressable)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Functional	Intersects With	Sensitive / Regulated Data Access Enforcement	CFG-08	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to restrict access to sensitive/regulated data.	5	
§ 164.312(c)(2)	Implementation specification: Mechanism to authenticate electronic protected health information (Addressable)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Functional	Intersects With	Sensitive / Regulated Data Actions	CFG-08.1	Automated mechanisms exist to generate event logs whenever sensitive/regulated data is collected, created, updated, deleted and/or archived.	5	
§ 164.312(c)(2)	Implementation specification: Mechanism to authenticate electronic protected health information (Addressable)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	5	
§ 164.312(c)(2)	Implementation specification: Mechanism to authenticate electronic protected health information (Addressable)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Functional	Intersects With	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.	5	
§ 164.312(c)(2)	Implementation specification: Mechanism to authenticate electronic protected health information (Addressable)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
§ 164.312(d)	Standard: Person or entity authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
§ 164.312(d)	Standard: Person or entity authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
§ 164.312(d)	Standard: Person or entity authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Functional	Intersects With	Identity Proofing (Identity Verification)	IAC-28	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	5	
§ 164.312(d)	Standard: Person or entity authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Functional	Intersects With	Identity Evidence	IAC-28.2	Mechanisms exist to require evidence of individual identification to be presented to the registration authority.	5	
§ 164.312(d)	Standard: Person or entity authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Functional	Intersects With	Identity Evidence Validation & Verification	IAC-28.3	Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification.	5	
§ 164.312(d)	Standard: Person or entity authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
§ 164.312(e)	Standard: Transmission security	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.312(e)(1)	N/A	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
§ 164.312(e)(1)	N/A	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
§ 164.312(e)(1)	N/A	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
§ 164.312(e)(2)	Implementation specifications:	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.312(e)(2)(i)	Integrity controls (Addressable)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
§ 164.312(e)(2)(i)	Integrity controls (Addressable)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
§ 164.312(e)(2)(i)	Integrity controls (Addressable)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
§ 164.312(e)(2)(ii)	Encryption (Addressable)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
§ 164.312(e)(2)(ii)	Encryption (Addressable)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
§ 164.312(e)(2)(ii)	Encryption (Addressable)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
§ 164.314	Organizational requirements	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.314(a)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.314(a)(1)	Standard: Business associate contracts or other arrangements	The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
§ 164.314(a)(2)	Implementation specifications (Required)	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.314(a)(2)(i)	Business associate contracts	The contract must provide that the business associate will—	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.314(a)(2)(i)(A)	N/A	Comply with the applicable requirements of this subpart;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.314(a)(2)(i)(B)	N/A	In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and	Functional	Equal	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	10	
§ 164.314(a)(2)(i)(C)	N/A	Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.	Functional	Equal	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	10	
§ 164.314(a)(2)(ii)	Other arrangements	The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
§ 164.314(a)(2)(iii)	Business associate contracts with subcontractors	The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
§ 164.314(a)(2)(iii)	Business associate contracts with subcontractors	The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
§ 164.314(b)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.314(b)(1)	Standard: Requirements for group health plans	Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Functional	Equal	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.314(b)(2)	Implementation specifications (Required)	The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.314(b)(2)(i)	N/A	Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;	Functional	Equal	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.314(b)(2)(ii)	N/A	Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;	Functional	Equal	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.314(b)(2)(iii)	N/A	Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and	Functional	Equal	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.314(b)(2)(iv)	N/A	Report to the group health plan any security incident of which it becomes aware.	Functional	Equal	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.316	Policies and procedures and documentation requirements	A covered entity or business associate must, in accordance with § 164.306:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.316(a)	Standard: Policies and procedures	Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
§ 164.316(a)	Standard: Policies and procedures	Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.316(b)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.316(b)(1)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.316(b)(1)(i)	Standard: Documentation	Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.316(b)(1)(ii)	N/A	If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	3	
§ 164.316(b)(1)(ii)	N/A	If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	3	
§ 164.316(b)(2)	Implementation specifications:	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.316(b)(2)(i)	Time limit (Required)	Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	Functional	Equal	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	
§ 164.316(b)(2)(ii)	Availability (Required)	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
§ 164.316(b)(2)(ii)	Availability (Required)	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
§ 164.316(b)(2)(iii)	Updates (Required)	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
§ 164.316(b)(2)(iii)	Updates (Required)	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
§ 164.318	Compliance dates for the initial implementation of the security standards	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.318(a)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.318(a)(1)	Health plan	A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than April 20, 2005.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.318(a)(2)	N/A	A small health plan must comply with the applicable requirements of this subpart no later than April 20, 2006.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.318(b)	Health care clearinghouse	A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 20, 2005.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.318(c)	Health care provider	A covered health care provider must comply with the applicable requirements of this subpart no later than April 20, 2005.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.400	Applicability	The requirements of this subpart shall apply with respect to breaches of protected health information occurring on or after September 23, 2009.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.402	Definitions	[see focal document for details]	Functional	Subset Of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
§ 164.404	Notification to individuals	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.404(a)	Standard	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.404(a)(1)	General rule	A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(a)(2)	Breaches treated as discovered	For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(b)	Implementation specification: Timeliness of notification	Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders; (2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
§ 164.404(c)	Implementation specifications: Content of notification	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.404(c)(1)	Elements	The notification required by paragraph (a) of this section shall include, to the extent possible:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.404(c)(1)(A)	N/A	A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(c)(1)(B)	N/A	A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(c)(1)(C)	N/A	Any steps individuals should take to protect themselves from potential harm resulting from the breach;	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(c)(1)(D)	N/A	A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(c)(1)(E)	N/A	Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(c)(2)	Plain language requirement	The notification required by paragraph (a)of this section shall be written in plain language.	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(d)	Implementation specifications: Methods of individual notification	The notification required by paragraph (a) of this section shall be provided in the following form:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.404(d)(1)	Written notice	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.404(d)(1)(i)	N/A	Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(d)(1)(ii)	N/A	If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under § 164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(d)(2)	Substitute notice	In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(d)(2)(i)	N/A	In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(d)(2)(ii)	N/A	In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.404(d)(2)(ii)(A)	N/A	Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.404(d)(2)(ii)(B)	N/A	Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.404(d)(3)	Additional notice in urgent situations	In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.406	Notification to the media	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.406(a)	Standard	For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in § 164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.406(b)	Implementation specification: Timeliness of notification	Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.406(c)	Implementation specifications: Content of notification	The notification required by paragraph (a) of this section shall meet the requirements of § 164.404(c).	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.408	Notification to the Secretary	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.408(a)	Standard	A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders; (2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
§ 164.408(b)	Implementation specifications: Breaches involving 500 or more individuals	For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS Web site.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders; (2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
§ 164.408(c)	Implementation specifications: Breaches involving less than 500 individuals	For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders; (2) Affected clients & third-parties; and(3) Regulatory authorities.	10	
§ 164.410	Notification by a business associate	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.410(a)	Standard	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.410(a)(1)	General rule	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
§ 164.410(a)(1)	General rule	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	Functional	Intersects With	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5	
§ 164.410(a)(2)	Breaches treated as discovered	For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).	Functional	Subset Of	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	10	
§ 164.410(b)	Implementation specifications: Timeliness of notification	Except as provided in § 164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.	Functional	Subset Of	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	10	
§ 164.410(c)	Implementation specifications: Content of notification	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.410(c)(1)	N/A	The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.	Functional	Subset Of	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	10	
§ 164.410(c)(2)	N/A	A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under § 164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	Functional	Subset Of	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	10	
§ 164.412	Law enforcement delay	If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
§ 164.412(a)	N/A	If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
§ 164.412(b)	N/A	If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
§ 164.414	Administrative requirements and burden of proof	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.414(a)	Administrative requirements	A covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.414(b)	Burden of proof	In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500	Applicability	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(a)	N/A	Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(b)	N/A	Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(b)(1)	N/A	When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(b)(1)(i)	N/A	Section 164.500 relating to applicability;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(b)(1)(ii)	N/A	Section 164.501 relating to definitions;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(b)(1)(iii)	N/A	Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(b)(1)(iv)	N/A	Section 164.504 relating to the organizational requirements for covered entities;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(b)(1)(v)	N/A	Section 164.512 relating to uses and disclosures for which individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(b)(1)(vi)	N/A	Section 164.532 relating to transition requirements; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(b)(1)(vii)	N/A	Section 164.534 relating to compliance dates for initial implementation of the privacy standards.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(b)(2)	N/A	When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(c)	N/A	Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.500(d)	N/A	The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or non-governmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.501	Definitions	[see focal document for details]	Functional	Subset Of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
§ 164.502	Uses and disclosures of protected health information: General rules	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.502(a)	Standard	A covered entity or business associate may not use or disclose protected health information except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.	Functional	Subset Of	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	10	
§ 164.502(a)	Standard	A covered entity or business associate may not use or disclose protected health information except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
§ 164.502(a)(1)	Covered entities: Permitted uses and disclosures	A covered entity is permitted to use or disclose protected health information as follows:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(1)(i)	N/A	To the individual;	Functional	Subset Of	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business	10	
§ 164.502(a)(1)(ii)	N/A	For treatment, payment, or healthcare operations, as permitted by and in compliance with § 164.506;	Functional	Subset Of	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business	10	
§ 164.502(a)(1)(iii)	N/A	Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;	Functional	Subset Of	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process.	10	
§ 164.502(a)(1)(iv)	N/A	Except for uses and disclosures prohibited under § 164.502(a)(5)(i), pursuant to and in compliance with valid authorization under § 164.508;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(1)(v)	N/A	Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(1)(vi)	N/A	As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(2)	Covered entities: Required disclosures	A covered entity is required to disclose protected health information:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(2)(i)	N/A	To an individual, when requested under, and required by § 164.524 or§ 164.528; and	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where	10	
§ 164.502(a)(2)(ii)	N/A	When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the	10	
§ 164.502(a)(3)	Business associates: Permitted uses and disclosures	A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.	Functional	Subset Of	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	10	
§ 164.502(a)(4)	Business associates: Required uses and disclosures	A business associate is required to disclose protected health information:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(4)(i)	N/A	When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.502(a)(4)(ii)	N/A	To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.502(a)(5)	Prohibited uses and disclosures	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(i)	Use and disclosure of genetic information for underwriting purposes:	Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:	Functional	Subset Of	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process.	10	
§ 164.502(a)(5)(i)(A)	N/A	Except as provided in paragraph (a)(5)(i)(B) of this section:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(i)(A)(1)	N/A	Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(i)(A)(2)	N/A	The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(i)(A)(3)	N/A	The application of any pre-existing condition exclusion under the plan, coverage, or policy; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(i)(A)(4)	N/A	Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(i)(B)	N/A	Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(ii)	Sale of protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(ii)(A)	N/A	Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.	Functional	Subset Of	Prohibition of Selling, Processing and/or Sharing Personal Data (PD)	PRI-03.3	Mechanisms exist to prevent the sale, processing and/or sharing of Personal Data (PD) when:(1) Instructed by the data subject; or(2) The data subject is a minor, where selling and/or sharing PD is legally prohibited.	10	
§ 164.502(a)(5)(ii)(B)	N/A	For purposes of this paragraph, sale of protected health information means:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(ii)(B)(1)	N/A	Except as provided in paragraph (a)(5)(ii)(B)(2) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(ii)(B)(2)	N/A	Sale of protected health information does not include a disclosure of protected health information:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(ii)(B)(2)(i)	N/A	For public health purposes pursuant to § 164.512(b) or § 164.514(e);	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(ii)(B)(2)(ii)	N/A	For research purposes pursuant t§ 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(ii)(B)(2)(iii)	N/A	For treatment and payment purposes pursuant to § 164.506(a);	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(ii)(B)(2)(iv)	N/A	For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(ii)(B)(2)(v)	N/A	To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(ii)(B)(2)(vi)	N/A	To an individual, when requested under § 164.524 or § 164.528;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(ii)(B)(2)(vii)	N/A	Required by law as permitted under § 164.512(a); and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(a)(5)(ii)(B)(2)(viii)	N/A	For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(b)	Standard: Minimum necessary	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(b)(1)	Minimum necessary applies	When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.	Functional	Subset Of	Minimize Sensitive / Regulated Data	DCH-18.1	Mechanisms exist to minimize sensitive/regulated data that is collected, received, processed, stored and/or transmitted throughout the information lifecycle to only those elements necessary to support necessary business processes.	10	
§ 164.502(b)(2)	Minimum necessary does not apply	This requirement does not apply to:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(b)(2)(i)	N/A	Disclosures to or requests by a health care provider for treatment;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(b)(2)(ii)	N/A	Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(b)(2)(iii)	N/A	Uses or disclosures made pursuant to an authorization under § 164.508;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(b)(2)(iv)	N/A	Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(b)(2)(v)	N/A	Uses or disclosures that are required by law, as described by § 164.512(a); and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(b)(2)(vi)	N/A	Uses or disclosures that are required for compliance with applicable requirements of this subchapter.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(c)	Standard: Uses and disclosures of protected health information subject to an agreed upon restriction	A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.502(d)	Standard: Uses and disclosures of de-identified protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.502(d)(1)	Uses and disclosures to create de-identified information	A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.502(d)(2)	Uses and disclosures of de-identified information	Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(d)(2)(i)	N/A	Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(d)(2)(ii)	N/A	If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(e)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(e)(1)	Standard: Disclosures to business associates	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(e)(1)(i)	N/A	A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
§ 164.502(e)(1)(i)	N/A	A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	Functional	Intersects With	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration(1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to subcontractors.	5	
§ 164.502(e)(1)(ii)	N/A	A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
§ 164.502(e)(1)(ii)	N/A	A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.	Functional	Intersects With	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration(1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to subcontractors.	5	
§ 164.502(e)(2)	Implementation specification: Documentation	The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.502(f)	Standard: Deceased individuals	A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(1)	Standard: Personal representatives	As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.	Functional	Subset Of	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity (e.g., authorized agent, proxy, etc.), acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	10	
§ 164.502(g)(2)	Implementation specification: adults and emancipated minors	If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.	Functional	Subset Of	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity (e.g., authorized agent, proxy, etc.), acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	10	
§ 164.502(g)(3)	Implementation specification: unemancipated minors	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(3)(i)	N/A	If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:	Functional	Subset Of	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity (e.g., authorized agent, proxy, etc.), acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	10	
§ 164.502(g)(3)(i)(A)	N/A	The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;	Functional	Subset Of	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity (e.g., authorized agent, proxy, etc.), acting on the data subject's behalf, to make Personal Data (PD) processing decisions.	10	
§ 164.502(g)(3)(i)(B)	N/A	The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(3)(i)(C)	N/A	A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(3)(ii)	N/A	Notwithstanding the provisions of paragraph (g)(3)(i) of this section:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(3)(ii)(A)	N/A	If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(3)(ii)(B)	N/A	If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(3)(ii)(C)	N/A	Where the parent, guardian, or other person acting in loco parentis, is not the personal representative under paragraphs (g)(3)(i)(A), (B), or(C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under § 164.524 to a parent, guardian, or other person acting in loco parentis, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(4)	Implementation specification: Deceased individuals	If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(5)	Implementation specification: Abuse, neglect, endangerment situations	Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative of an individual if:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(5)(i)	N/A	The covered entity has a reasonable belief that:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(5)(i)(A)	N/A	The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(5)(i)(B)	N/A	Treating such person as the personal representative could endanger the individual; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(g)(5)(ii)	N/A	The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(h)	Standard: Confidential communications	A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(i)	Standard: Uses and disclosures consistent with notice	A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.	Functional	Subset Of	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process.	10	
§ 164.502(j)	Standard: Disclosures by whistleblowers and workforce member crime victims	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(j)(1)	Disclosures by whistleblowers	A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(j)(1)(i)	N/A	The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(j)(1)(ii)	N/A	The disclosure is to:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.502(j)(1)(iii)(A)	N/A	A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(j)(1)(ii)(B)	N/A	An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(j)(2)	Disclosures by workforce members who are victims of a crime	A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(j)(2)(i)	N/A	The protected health information disclosed is about the suspected perpetrator of the criminal act; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.502(j)(2)(ii)	N/A	The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504	Uses and disclosures: Organizational requirements	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(a)	Definitions	[see focal document for details]	Functional	Subset Of	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	10	
§ 164.504(b)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(c)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(d)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(1)	Standard: Business associate contracts	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(1)(i)	N/D324:E326	The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(1)(ii)	N/A	A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(1)(iii)	N/A	A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(2)	Implementation specifications: Business associate contracts	A contract between the covered entity and a business associate must:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(2)(i)	N/A	Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
§ 164.504(e)(2)(i)	N/A	Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(e)(2)(i)(A)	N/A	The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(e)(2)(i)(B)	N/A	The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(e)(2)(ii)	N/A	Provide that the business associate will:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(2)(ii)(A)	N/A	Not use or further disclose the information other than as permitted or required by the contract or as required by law;	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
§ 164.504(e)(2)(ii)(B)	N/A	Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
§ 164.504(e)(2)(ii)(C)	N/A	Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
§ 164.504(e)(2)(ii)(D)	N/A	In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;	Functional	Subset Of	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	10	
§ 164.504(e)(2)(ii)(E)	N/A	Make available protected health information in accordance with § 164.524;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(2)(ii)(F)	N/A	Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(2)(ii)(G)	N/A	Make available the information required to provide an accounting of disclosures in accordance with § 164.528;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(2)(ii)(H)	N/A	To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(2)(ii)(I)	N/A	Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(2)(ii)(J)	N/A	At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(e)(2)(iii)	N/A	Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.	Functional	Equal	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	10	
§ 164.504(e)(3)	Implementation specifications: Other arrangements	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(3)(i)	N/A	If a covered entity and its business associate are both governmental entities:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(3)(i)(A)	N/A	The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(3)(i)(B)	N/A	The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(3)(ii)	N/A	If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(3)(iii)	N/A	The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(3)(iv)	N/A	A covered entity may comply with this paragraph and § 164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the covered entity has a data use agreement with the business associate that complies with § 164.514(e)(4) and § 164.314(a)(1), if applicable.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.504(e)(4)	Implementation specifications: Other requirements for contracts and other arrangements	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(4)(i)	N/A	The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to the covered entity, if necessary:	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
§ 164.504(e)(4)(i)(A)	N/A	For the proper management and administration of the business associate; or	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
§ 164.504(e)(4)(i)(B)	N/A	To carry out the legal responsibilities of the business associate.	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
§ 164.504(e)(4)(i)(B)(ii)	N/A	The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
§ 164.504(e)(4)(i)(B)(ii)(A)	N/A	The disclosure is required by law; or	Functional	Subset Of	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	10	
§ 164.504(e)(4)(i)(B)(ii)(B)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(e)(4)(i)(B)(ii)(B)(1)	N/A	The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(e)(4)(i)(B)(ii)(B)(2)	N/A	The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(e)(5)	Implementation specifications: Business associate contracts with subcontractors	The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)(1)	Standard: Requirements for group health plans	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)(1)(i)	N/A	Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(1)(ii)	N/A	Except as prohibited by § 164.502(a)(5)(i), the group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for purposes of:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)(1)(ii)(A)	N/A	Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)(1)(ii)(B)	N/A	Modifying, amending, or terminating the group health plan.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)(1)(iii)	N/A	The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)(2)	Implementation specifications: Requirements for plan documents	The plan documents of the group health plan must be amended to incorporate provisions to:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)(2)(i)	N/A	Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(ii)	N/A	Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(ii)(A)	N/A	Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(ii)(B)	N/A	Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(ii)(C)	N/A	Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(ii)(D)	N/A	Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(ii)(E)	N/A	Make available protected health information in accordance with § 164.524;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(ii)(F)	N/A	Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(ii)(G)	N/A	Make available the information required to provide an accounting of disclosures in accordance with § 164.528;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(ii)(H)	N/A	Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(ii)(I)	N/A	If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(ii)(J)	N/A	Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(iii)	N/A	Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)(2)(iii)	N/A	Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)(2)(iii)	N/A	Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)(2)(iii)	N/A	Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)(2)(iii)(A)	N/A	Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(iii)(B)	N/A	Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(2)(iii)(C)	N/A	Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(3)	Implementation specifications: Uses and disclosures	A group health plan may:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(f)(3)(i)	N/A	Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(3)(ii)	N/A	Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(3)(iii)	N/A	Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
§ 164.504(f)(3)(iv)	N/A	Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.504(g)	Standard: Requirements for a covered entity with multiple covered functions	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.504(g)(1)	N/A	A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
§ 164.504(g)(2)	N/A	A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.506	Uses and disclosures to carry out treatment, payment, or health care operations	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.506(a)	Standard: Permitted uses and disclosures	Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) through (4) or that are prohibited under § 164.502(a)(5)(ii), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.506(b)	Standard: Consent for uses and disclosures permitted	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.506(b)(1)	N/A	A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
§ 164.506(b)(2)	N/A	Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under § 164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.506(c)	Implementation specifications: Treatment, payment, or health care operations	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.506(c)(1)	N/A	A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.506(c)(1)	N/A	A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.	Functional	Subset Of	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	10	
§ 164.506(c)(2)	N/A	A covered entity may disclose protected health information for treatment activities of a health care provider.	Functional	Subset Of	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	10	
§ 164.506(c)(3)	N/A	A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.	Functional	Subset Of	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	10	
§ 164.506(c)(4)	N/A	A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:	Functional	Subset Of	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	10	
§ 164.506(c)(4)(i)	N/A	For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.506(c)(4)(ii)	N/A	For the purpose of health care fraud and abuse detection or compliance.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.506(c)(5)	N/A	A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.508	Uses and disclosures for which an authorization is required	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(a)	Standard: Authorizations for useand disclosures —	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(a)(1)	Authorization required: General rule	Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.508(a)(1)	Authorization required: General rule	Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.	Functional	Subset Of	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	10	
§ 164.508(a)(2)	Authorization required: Psychotherapy notes	Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
§ 164.508(a)(2)(i)	N/A	To carry out the following treatment, payment, or health care operations:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(a)(2)(i)(A)	N/A	Use by the originator of the psychotherapy notes for treatment;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(a)(2)(i)(B)	N/A	Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or	Functional	Subset Of	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that:(1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and(2) Authorizes the use of PD when such information is required for internal testing, training and research.	10	
§ 164.508(a)(2)(i)(C)	N/A	Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.508(a)(2)(ii)	N/A	A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; 164.512(g)(1); or 164.512(j)(1)(i).	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(a)(3)	Authorization required: Marketing	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(a)(3)(i)	N/A	Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization or any use for disclosure of protected health information for marketing, except if the communication is in the form of:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(a)(3)(i)(A)	N/A	A face-to-face communication made by a covered entity to an individual; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(a)(3)(i)(B)	N/A	A promotional gift of nominal value provided by the covered entity	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(a)(3)(ii)	N/A	If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(a)(4)	Authorization required: Sale of protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(a)(4)(i)	N/A	Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart.	Functional	Subset Of	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	10	
§ 164.508(a)(4)(ii)	N/A	Such authorization must state that the disclosure will result in remuneration to the covered entity.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)	Implementation specifications: General requirements	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(1)	Valid authorizations	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(1)(i)	N/A	A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(ii), (c)(1), and (c)(2) of this section, as applicable.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(1)(ii)	N/A	A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(2)	Defective authorizations	An authorization is not valid, if the document submitted has any of the following defects:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(2)(i)	N/A	The expiration date has passed or the expiration event is known by the covered entity to have occurred;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(2)(ii)	N/A	The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(2)(iii)	N/A	The authorization is known by the covered entity to have been revoked;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(2)(iv)	N/A	The authorization violates paragraph (b)(3) or (4) of this section, if applicable;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(2)(v)	N/A	Any material information in the authorization is known by the covered entity to be false.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.508(b)(3)	Compound authorizations	An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(3)(i)	N/A	An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(3)(ii)	N/A	An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(3)(iii)	N/A	An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(4)	Prohibition on conditioning of authorizations	A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(4)(i)	N/A	A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(4)(ii)	N/A	A health plan may condition enrollment in the health plan or eligibility for benefits on provision an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(4)(ii)(A)	N/A	The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(4)(ii)(B)	N/A	The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(4)(iii)	N/A	A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(5)	Revocation of authorizations	An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(5)(i)	N/A	The covered entity has taken action in reliance thereon; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(5)(ii)	N/A	If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(b)(6)	Documentation	A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(c)	Implementation specifications: Core elements and requirements	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(c)(1)	Core elements	A valid authorization under this section must contain at least the following elements:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(c)(1)(i)	N/A	A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.	Functional	Subset Of	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	10	
§ 164.508(c)(1)(ii)	N/A	The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.	Functional	Subset Of	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	10	
§ 164.508(c)(1)(iii)	N/A	The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.	Functional	Subset Of	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	10	
§ 164.508(c)(1)(iv)	N/A	A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.	Functional	Subset Of	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	10	
§ 164.508(c)(1)(v)	N/A	An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
§ 164.508(c)(1)(vi)	Signature of the individual and date	If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(c)(2)	Required statements	In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(c)(2)(i)	N/A	The individual's right to revoke the authorization in writing, and either:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(c)(2)(i)(A)	N/A	The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or	Functional	Subset Of	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	10	
§ 164.508(c)(2)(i)(B)	N/A	To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.	Functional	Subset Of	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	10	
§ 164.508(c)(2)(ii)	N/A	The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(c)(2)(ii)(A)	N/A	The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or	Functional	Subset Of	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting: (1) Refusing products and/or services;(2) Charging different rates for goods and/or services; and(3) Providing different levels of quality.	10	
§ 164.508(c)(2)(ii)(B)	N/A	The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.	Functional	Subset Of	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting: (1) Refusing products and/or services;(2) Charging different rates for goods and/or services; and(3) Providing different levels of quality.	10	
§ 164.508(c)(2)(iii)	N/A	The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.508(c)(3)	Plain language requirement	The authorization must be written in plain language.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
§ 164.508(c)(4)	Copy to the individual	If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510	Uses and disclosures requiring an opportunity for the individual to agree or to object	A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(a)	Standard: Use and disclosure for facility directories	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(a)(1)	Permitted uses and disclosure	Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(a)(1)(i)	N/A	Use the following protected health information to maintain a directory of individuals in its facility:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(a)(1)(i)(A)	N/A	The individual's name;	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.510(a)(1)(i)(B)	N/A	The individual's location in the covered health care provider's facility;	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.510(a)(1)(i)(C)	N/A	The individual's condition described in general terms that does not communicate specific medical information about the individual; and	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.510(a)(1)(i)(D)	N/A	The individual's religious affiliation; and	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.510(a)(1)(ii)	N/A	Use or disclose for directory purposes such information:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(a)(1)(ii)(A)	N/A	To members of the clergy; or	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.510(a)(1)(ii)(B)	N/A	Except for religious affiliation, to other persons who ask for the individual by name.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.510(a)(2)	Opportunity to object	A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(a)(3)	Emergency circumstances	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(a)(3)(i)	N/A	If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(a)(3)(i)(A)	N/A	Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(a)(3)(i)(B)	N/A	In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(a)(3)(ii)	N/A	The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it become practicable to do so.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(b)	Standard: Uses and disclosures for involvement in the individual's care and notification purposes	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(b)(1)	Permitted uses and disclosures	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.510(b)(1)(i)	N/A	A covered entity may, in accordance with paragraphs (b)(2), (b)(3), or (b)(5) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.510(b)(1)(ii)	N/A	A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating),a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (b)(3), (b)(4), or (b)(5) of this section, as applicable.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.510(b)(2)	Uses and disclosures with the individual present	If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.510(b)(2)(i)	N/A	Obtains the individual's agreement;	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
§ 164.510(b)(2)(ii)	N/A	Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
§ 164.510(b)(2)(iii)	N/A	Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
§ 164.510(b)(3)	Limited uses and disclosures when the individual is not present	If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
§ 164.510(b)(4)	Uses and disclosures for disaster relief purposes	A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.510(b)(4)	Uses and disclosures for disaster relief purposes	A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.510(b)(5)	Uses and disclosures when the individual is deceased	If the individual is deceased, a covered entity may disclose to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512	Uses and disclosures for which an authorization or opportunity to agree or object is not required	A covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512	Uses and disclosures for which an authorization or opportunity to agree or object is not required	A covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given orally.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(a)	Standard: Uses and disclosures required by law	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(a)(1)	N/A	A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(a)(2)	N/A	A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)	Standard: Uses and disclosures for public health activities	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)	N/A	A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(i)	Permitted uses and disclosures	A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(ii)	N/A	A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.512(b)(1)(iii)	N/A	A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(iii)(A)	N/A	To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(iii)(B)	N/A	To track FDA-regulated products;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(iii)(C)	N/A	To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(iii)(D)	N/A	To conduct post marketing surveillance;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(iv)	N/A	A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(v)	N/A	An employer, about an individual who is a member of the workforce of the employer, if:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(v)(A)	N/A	The covered entity is a covered health care provider who provides health care to the individual at the request of the employer:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(v)(A)(1)	N/A	To conduct an evaluation relating to medical surveillance of the workplace; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(v)(A)(2)	N/A	To evaluate whether the individual has a work-related illness or injury;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(v)(B)	N/A	The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(v)(C)	N/A	The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(v)(D)	N/A	The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(v)(D)(1)	N/A	By giving a copy of the notice to the individual at the time the health care is provided; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(v)(D)(2)	N/A	If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(vi)	N/A	A school, about an individual who is a student or prospective student of the school, if:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(vi)(A)	N/A	The protected health information that is disclosed is limited to proof of immunization;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(vi)(B)	N/A	The school is required by State or other law to have such proof of immunization prior to admitting the individual; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(vi)(C)	N/A	The covered entity obtains and documents the agreement to the disclosure from either:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(vi)(C)(1)	N/A	A parent, guardian, or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(1)(vi)(C)(2)	N/A	The individual, if the individual is an adult or emancipated minor.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(b)(2)	Permitted uses	If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(c)	Standard: Disclosures about victims of abuse, neglect or domestic violence	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(c)(1)	Permitted disclosures	Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(c)(1)(i)	N/A	To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(c)(1)(ii)	N/A	If the individual agrees to the disclosure; or	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(c)(1)(iii)	N/A	To the extent the disclosure is expressly authorized by statute or regulation and:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(c)(1)(iii)(A)	N/A	The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(c)(1)(iii)(B)	N/A	If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(c)(2)	Informing the individual	A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(c)(2)(i)	N/A	The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(c)(2)(ii)	N/A	The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(d)	Standard: Uses and disclosures for health oversight activities	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(d)(1)	Permitted disclosures	A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(d)(1)(i)	N/A	The health care system;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(d)(1)(ii)	N/A	Government benefit programs for which health information is relevant to beneficiary eligibility;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(d)(1)(iii)	N/A	Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(d)(1)(iv)	N/A	Entities subject to civil rights laws for which health information is necessary for determining compliance.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(d)(2)	Exception to health oversight activities	For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(d)(2)(i)	N/A	The receipt of health care;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(d)(2)(ii)	N/A	A claim for public benefits related to health; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(d)(2)(iii)	N/A	Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(d)(3)	Joint activities or investigations	Notwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(d)(4)	Permitted uses	If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(e)	Standard: Disclosures for judicial and administrative proceedings	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(e)(1)	Permitted disclosures	A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(i)	N/A	In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(ii)	N/A	In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(ii)(A)	N/A	The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.512(e)(1)(ii)(B)	N/A	The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(iii)	N/A	For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(iii)(A)	N/A	The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(iii)(B)	N/A	The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(iii)(C)	N/A	The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(iii)(C)(1)	N/A	No objections were filed; or	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(iii)(C)(2)	N/A	All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(iv)	N/A	For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information , if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(iv)(A)	N/A	The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(iv)(B)	N/A	The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(v)	N/A	For purposes of paragraph (e)(1) of this section, a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(v)(A)	N/A	Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(v)(B)	N/A	Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(1)(vi)	N/A	Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(iv) of this section.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(e)(2)	Other uses and disclosures under this section	The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(f)	Standard: Disclosures for law enforcement purposes	A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(1)	Permitted disclosures: Pursuant to process and as otherwise required by law	A covered entity may disclose protected health information:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(1)(i)	N/A	As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(1)(ii)	N/A	In compliance with and as limited by the relevant requirements of:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(f)(1)(ii)(A)	N/A	A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(1)(ii)(B)	N/A	A grand jury subpoena; or	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(1)(ii)(C)	N/A	An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(1)(ii)(C)(1)	N/A	The information sought is relevant and material to a legitimate law enforcement inquiry;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(1)(ii)(C)(2)	N/A	The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(1)(ii)(C)(3)	N/A	De-identified information could not reasonably be used.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(2)	N/A	Permitted disclosures: Limited information for identification and location purposes. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(2)(i)	N/A	The covered entity may disclose only the following information:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(f)(2)(i)(A)	N/A	Name and address;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(2)(i)(B)	N/A	Date and place of birth;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(2)(i)(C)	N/A	Social security number;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(2)(i)(D)	N/A	ABO blood type and rh factor;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(2)(i)(E)	N/A	Type of injury;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(2)(i)(F)	N/A	Date and time of treatment;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(2)(i)(G)	N/A	Date and time of death, if applicable; and	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(2)(i)(H)	N/A	A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(2)(ii)	N/A	Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(3)	Permitted disclosure: Victims of a crime	Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individualwho is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(3)(i)	N/A	The individual agrees to the disclosure; or	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(3)(ii)	N/A	The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(3)(ii)(A)	N/A	The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(3)(ii)(B)	N/A	The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(3)(ii)(C)	N/A	The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(4)	Permitted disclosure: Decedents	A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(5)	Permitted disclosure: Crime on premises	A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(6)	Permitted disclosure: Reporting crime in emergencies	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(f)(6)(i)	N/A	A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(6)(i)(A)	N/A	The commission and nature of a crime;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.512(f)(6)(i)(B)	N/A	The location of such crime or of the victim(s) of such crime; and	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(6)(i)(C)	N/A	The identity, description, and location of the perpetrator of such crime.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(f)(6)(ii)	N/A	If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(g)	Standard: Uses and disclosures about decedents	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(g)(1)	Coroners and medical examiners	A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(g)(2)	Funeral directors	A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(h)	Standard: Uses and disclosures for cadaveric organ, eye or tissue donation purposes	A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(i)	Standard: Uses and disclosures for research purposes	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(1)	Permitted uses and disclosures	A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(i)(1)	Permitted uses and disclosures	A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the [illegible]	10	
§ 164.512(i)(1)(i)	Board approval of a waiver of authorization	The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by § 164.508 for use or disclosure of protected health information has been approved by either:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(1)(i)(A)	N/A	An Institutional Review Board (IRB), established in accordance with 7 CFR lc.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 6.107, 45 CFR 690.107, or 49 CFR 11.107; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(1)(i)(B)	N/A	A privacy board that:	Functional	Subset Of	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	10	
§ 164.512(i)(1)(i)(B)(1)	N/A	Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;	Functional	Subset Of	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	10	
§ 164.512(i)(1)(i)(B)(2)	N/A	Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and	Functional	Subset Of	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	10	
§ 164.512(i)(1)(i)(B)(3)	N/A	Does not have any member, participating in a review of any project in which the member has a conflict of interest.	Functional	Subset Of	Data Quality Management	PRI-10	Mechanisms exist to manage the quality, utility, objectivity, integrity and impact determination and de-identification of sensitive/regulated data across the information lifecycle.	10	
§ 164.512(i)(1)(ii)	Reviews preparatory to research	The covered entity obtains from the researcher representations that:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(1)(ii)(A)	N/A	Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(1)(ii)(B)	N/A	No protected health information is to be removed from the covered entity by the researcher in the course of the review; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(1)(ii)(C)	N/A	The protected health information for which use or access is sought is necessary for the research purposes.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(1)(iii)	Research on decedent's information	The covered entity obtains from the researcher:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(1)(iii)(A)	N/A	Representation that the use or disclosure sought is solely for research on the protected health information of decedents;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(1)(iii)(B)	N/A	Documentation, at the request of the covered entity, of the death of such individuals; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(1)(iii)(C)	N/A	Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)	Documentation of waiver approval	For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(i)	Identification and date of action	A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(ii)	Waiver criteria	A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(ii)(A)	N/A	The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(ii)(A)(1)	N/A	An adequate plan to protect the identifiers from improper use and disclosure;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(ii)(A)(2)	N/A	An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(ii)(A)(3)	N/A	Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(ii)(B)	N/A	The research could not practicably be conducted without the waiver or alteration; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(ii)(C)	N/A	The research could not practicably be conducted without access to and use of the protected health information.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(iii)	Protected health information needed	A brief description of the protected health information for which use or access has been determined to be necessary by the institutional review board or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(iv)	Review and approval procedures	A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(iv)(A)	N/A	An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b),38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR11.110);	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(iv)(B)	N/A	A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(iv)(C)	N/A	A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(i)(2)(v)	Required signature	The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(j)	Standard: Uses and disclosures to avert a serious threat to health or safety	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(j)(1)	Permitted disclosures	A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.512(j)(1)	Permitted disclosures	A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulatory and contractual obligations	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.512(j)(1)(i)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(j)(1)(i)(A)	N/A	Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(j)(1)(i)(B)	N/A	Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(j)(1)(ii)	N/A	Is necessary for law enforcement authorities to identify or apprehend an individual:	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(j)(1)(ii)(A)	N/A	Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(j)(1)(ii)(B)	N/A	Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(j)(2)	Use or disclosure not permitted	A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(j)(2)(i)	N/A	In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(j)(2)(ii)	N/A	Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(j)(3)	Limit on information that may be disclosed	A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(j)(4)	Presumption of good faith belief	A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(k)	Standard: Uses and disclosures for specialized government functions	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(k)(1)	Military and veterans activities	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(k)(1)(i)	Armed Forces personnel	A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the FEDERAL REGISTER the following information:	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(k)(1)(i)(A)	N/A	Appropriate military command authorities; and	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(k)(1)(i)(B)	N/A	The purposes for which the protected health information may be used or disclosed.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(k)(1)(ii)	Separation or discharge from military service	A covered entity that is a component of the Departments of Defense or Homeland Security may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(k)(1)(iii)	Veterans	A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(k)(1)(iv)	Foreign military personnel	A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the FEDERAL REGISTER pursuant to paragraph (k)(1)(i) of this section.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(k)(2)	National security and intelligence activities	A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(k)(3)	Protective services for the President and others	A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(k)(4)	Medical suitability determinations	A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(k)(4)(i)	N/A	For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12968;	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(k)(4)(ii)	N/A	As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(k)(4)(iii)	N/A	For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(k)(5)	Correctional institutions and other law enforcement custodial situations	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(k)(5)(i)	Permitted disclosures	A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(k)(5)(i)(A)	N/A	The provision of health care to such individuals;	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(k)(5)(i)(B)	N/A	The health and safety of such individual or other inmates;	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(k)(5)(i)(C)	N/A	The health and safety of the officers or employees of or others at the correctional institution;	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(k)(5)(i)(D)	N/A	The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(k)(5)(i)(E)	N/A	Law enforcement on the premises of the correctional institution; or	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(k)(5)(i)(F)	N/A	The administration and maintenance of the safety, security, and good order of the correctionalinstitution.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(k)(5)(ii)	Permitted uses	A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(k)(5)(iii)	No application after release	For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.512(k)(6)	Covered entities that are government programs providing public benefits	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.512(k)(6)(i)	N/A	A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.512(k)(6)(ii)	N/A	A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.512(k)(6)(ii)(1)	Standard: Disclosures for workers' compensation	A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.514	Other requirements relating to uses and disclosures of protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(a)	Standard: De-identification of protected health information	Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)	Implementation specifications: Requirements for de-identification of protected health information	A covered entity may determine that health information is not individually identifiable health information only if:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(1)	N/A	A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(1)(i)	N/A	Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(1)(ii)	N/A	Documents the methods and results of the analysis that justify such determination; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)	N/A	The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(A)	N/A	Names;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(B)	N/A	All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(B)(1)	N/A	The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(B)(2)	N/A	The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(C)	N/A	All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(D)	N/A	Telephone numbers;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(E)	N/A	Fax numbers;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(F)	N/A	Electronic mail addresses;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(G)	N/A	Social security numbers;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(H)	N/A	Medical record numbers;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(I)	N/A	Health plan beneficiary numbers;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(J)	N/A	Account numbers;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(K)	N/A	Certificate/license numbers;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(L)	N/A	Vehicle identifiers and serial numbers, including license plate numbers;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(M)	N/A	Device identifiers and serial numbers;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(N)	N/A	Web Universal Resource Locators (URLs);	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(O)	N/A	Internet Protocol (IP) address numbers;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(P)	N/A	Biometric identifiers, including finger and voice prints;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(Q)	N/A	Full face photographic images and any comparable images; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(i)(R)	N/A	Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c)of this section; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(b)(2)(ii)	N/A	The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(c)	Implementation specifications: Re-identification	A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(c)(1)	Derivation	The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(c)(2)	Security	The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for reidentification.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(d)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(d)(1)	Standard: Minimum necessary requirements	In order to comply with § 164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(d)(2)	Implementation specifications: Minimum necessary uses of protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(d)(2)(i)	N/A	A covered entity must identify:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(d)(2)(i)(A)	N/A	Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and	Functional	Subset Of	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	10	
§ 164.514(d)(2)(i)(B)	N/A	For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.	Functional	Subset Of	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	10	
§ 164.514(d)(2)(ii)	N/A	A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.	Functional	Subset Of	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	10	
§ 164.514(d)(3)	Implementation specification: Minimum necessary disclosures of protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(d)(3)(i)	N/A	For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
§ 164.514(d)(3)(i)	N/A	For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.	Functional	Subset Of	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	10	
§ 164.514(d)(3)(i)	N/A	For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(3)(ii)	N/A	For all other disclosures, a covered entity must:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(d)(3)(ii)(A)	N/A	Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(3)(ii)(B)	N/A	Review requests for disclosure on an individual basis in accordance with such criteria.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(3)(iii)	N/A	A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(3)(iii)(A)	N/A	Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(3)(iii)(B)	N/A	The information is requested by another covered entity;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(3)(iii)(C)	N/A	The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(3)(iii)(D)	N/A	Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(4)	N/A	Implementation specifications: Minimum necessary requests for protected health information	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(4)(i)	N/A	A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(4)(ii)	N/A	For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(4)(iii)	N/A	For all other requests, a covered entity must:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.514(d)(4)(iii)(A)	N/A	Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(4)(iii)(B)	N/A	Review requests for disclosure on an individual basis in accordance with such criteria.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(d)(5)	Implementation specification: Other content requirement	For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(e)(1)	Standard: Limited data set	A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)	Implementation specification: Limited data set	A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(i)	N/A	Names;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(ii)	N/A	Postal address information, other than town or city, State, and zip code;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(iii)	N/A	Telephone numbers;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(iv)	N/A	Fax numbers;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(v)	N/A	Electronic mail addresses;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(vi)	N/A	Social security numbers;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(vii)	N/A	Medical record numbers;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(viii)	N/A	Health plan beneficiary numbers;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(ix)	N/A	Account numbers;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(x)	N/A	Certificate/license numbers;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(xi)	N/A	Vehicle identifiers and serial numbers, including license plate numbers;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(xii)	N/A	Device identifiers and serial numbers;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(xiii)	N/A	Web Universal Resource Locators (URLs);	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(xiv)	N/A	Internet Protocol (IP) address numbers;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(xv)	N/A	Biometric identifiers, including finger and voice prints; and	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(2)(xvi)	N/A	Full face photographic images and any comparable images.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(3)	Implementation specification: Permitted purposes for uses and disclosures	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(e)(3)(i)	N/A	A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(3)(ii)	N/A	A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(4)	Implementation specifications: Data use agreement	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(e)(4)(i)	Agreement required	A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(4)(ii)	Contents	A data use agreement between the covered entity and the limited data set recipient must:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(4)(ii)(A)	N/A	Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(4)(ii)(B)	N/A	Establish who is permitted to use or receive the limited data set; and	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(4)(ii)(C)	N/A	Provide that the limited data set recipient will:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(4)(ii)(C)(1)	N/A	Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(4)(ii)(C)(2)	N/A	Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(4)(ii)(C)(3)	N/A	Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(4)(ii)(C)(4)	N/A	Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(4)(ii)(C)(5)	N/A	Not identify the information or contact the individuals.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.514(e)(4)(iii)	Compliance	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(e)(4)(iii)(A)	N/A	A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(e)(4)(iii)(A)(1)	N/A	Discontinued disclosure of protected health information to the recipient; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(e)(4)(iii)(A)(2)	N/A	Reported the problem to the Secretary.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(e)(4)(iii)(B)	N/A	A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(f)	Fundraising communications	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(f)(1)	N/A	Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(f)(1)(i)	N/A	Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(f)(1)(ii)	N/A	Dates of health care provided to an individual;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(f)(1)(iii)	N/A	Department of service information;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(f)(1)(iv)	N/A	Treating physician;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(f)(1)(v)	N/A	Outcome information; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(f)(1)(vi)	N/A	Health insurance status.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(f)(2)	Implementation specifications: Fundraising requirements	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(f)(2)(i)	N/A	A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(A) is included in the covered entity's notice of privacy practices.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.514(f)(2)(ii)	N/A	With each fundraising communication made to an individual under this paragraph, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
§ 164.514(f)(2)(iii)	N/A	A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.	Functional	Subset Of	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prevent discrimination against a data subject for exercising their legal rights pertaining to modifying or revoking consent, including prohibiting: (1) Refusing products and/or services;(2) Charging different rates for goods and/or [illegible]	10	
§ 164.514(f)(2)(iv)	N/A	A covered entity may not make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications under paragraph (f)(2)(ii) of this section.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	
§ 164.514(f)(2)(v)	N/A	A covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.	Functional	Subset Of	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:(1) Plain language to illustrate the potential data privacy risks of the authorization;(2) A means for users to decline the authorization; and(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.514(g)	Standard: Uses and disclosures for underwriting and related purposes	If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such protected health information for such purpose or as may be required by law, subject to the prohibition at § 164.502(a)(5)(i) with respect to genetic information included in the protected health information.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.514(h)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(1)	Standard: Verification requirements	Prior to any disclosure permitted by this subpart, a covered entity must:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(1)(i)	N/A	Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5)	10	
§ 164.514(h)(1)(ii)	N/A	Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the	10	
§ 164.514(h)(2)	Implementation specifications: Verification	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(2)(i)	Conditions on disclosures	If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(2)(i)(A)	N/A	The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(2)(i)(B)	N/A	The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(2)(ii)	Identity of public officials	A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(2)(ii)(A)	N/A	If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(2)(ii)(B)	N/A	If the request is in writing, the request is on the appropriate government letterhead; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(2)(ii)(C)	N/A	If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(2)(iii)	Authority of public officials	A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(2)(iii)(A)	N/A	A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(2)(iii)(B)	N/A	If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.514(h)(2)(iv)	Exercise of professional judgment	The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520	Notice of privacy practices for protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(a)	Standard: notice of privacy practices,	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(a)(1)	Right to notice	Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(a)(2)	Exception for group health plans	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(a)(2)(i)	N/A	An individual enrolled in a group health plan has a right to notice:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(a)(2)(i)(A)	N/A	From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(a)(2)(i)(B)	N/A	From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(a)(2)(ii)	N/A	A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(a)(2)(ii)(A)	N/A	Maintain a notice under this section; and	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.520(a)(2)(ii)(B)	N/A	Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(a)(2)(iii)	N/A	A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(a)(3)	Exception for inmates	An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(b)	Implementation specifications: Content of notice	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(b)(1)	Required elements	The covered entity must provide a notice that is written in plain language and that contains the elements required by this paragraph.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(i)	Header	The notice must contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(ii)	Uses and disclosures	The notice must contain:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(ii)(A)	N/A	A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(ii)(B)	N/A	A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(ii)(C)	N/A	If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202 of this subchapter.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(ii)(D)	N/A	For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(ii)(E)	N/A	A description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)-(a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by § 164.508(b)(5).	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(iii)	Separate statements for certain uses or disclosures	If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement informing the individual of such activities, as applicable:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(b)(1)(iii)(A)	N/A	In accordance with § 164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the individual has a right to opt out of receiving such communications;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(b)(1)(iii)(B)	N/A	In accordance with § 164.504(f), the group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(b)(1)(iii)(C)	N/A	If a covered entity that is a health plan, excluding an issuer of a long term care policy falling within paragraph (1)(viii) of the definition of health plan, intends to use or disclose protected health information for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(b)(1)(iv)	Individual rights	The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.520(b)(1)(iv)(A)	N/A	The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction, except in case of a disclosure restricted under § 164.522(a)(1)(vi);	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(iv)(B)	N/A	The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable;	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(iv)(C)	N/A	The right to inspect and copy protected health information as provided by § 164.524;	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(iv)(D)	N/A	The right to amend protected health information as provided by § 164.526;	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(iv)(E)	N/A	The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(iv)(F)	N/A	The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(v)	Covered entity's duties	The notice must contain:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(v)(A)	N/A	A statement that the covered entity is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information;	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(v)(B)	N/A	A statement that the covered entity is required to abide by the terms of the notice currently in effect; and	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(v)(C)	N/A	For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(vi)	Complaints	The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(vii)	Contact	The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by § 164.530(a)(1)(ii).	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(1)(viii)	Effective date	The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(2)	Optional elements	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.520(b)(2)(i)	N/A	In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i).	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(2)(ii)	N/A	For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(b)(3)	Revisions to the notice	The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(c)	Implementation specifications: Provision of notice	A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(c)(1)	Specific requirements for health plans	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(1)(i)	N/A	A health plan must provide the notice:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(c)(1)(i)(A)	N/A	No later than the compliance date for the health plan, to individuals then covered by the plan;	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(c)(1)(i)(B)	N/A	Thereafter, at the time of enrollment, to individuals who are new enrollees.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(c)(1)(ii)	N/A	No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(c)(1)(iii)	N/A	The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(c)(1)(iv)	N/A	If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(c)(1)(v)	N/A	If there is a material change to the notice:	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(c)(1)(v)(A)	N/A	A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.520(c)(1)(v)(B)	N/A	A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.520(c)(2)	Specific requirements for certain covered health care providers	A covered health care provider that has a direct treatment relationship with an individual must:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(2)(i)	Provide the notice:	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(2)(i)(A)	N/A	No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(2)(i)(B)	N/A	In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(2)(ii)	N/A	Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(2)(iii)	N/A	If the covered health care provider maintains a physical service delivery site:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(2)(iii)(A)	N/A	Have the notice available at the service delivery site for individuals to request to take with them; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(2)(iii)(B)	N/A	Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(2)(iv)	N/A	Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(3)	Specific requirements for electronic notice	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(3)(i)	N/A	A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(3)(ii)	N/A	A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the email transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(3)(iii)	N/A	For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(c)(3)(iv)	N/A	The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(d)	Implementation specifications: Joint notice by separate covered entities	Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(d)(1)	N/A	The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(d)(2)	N/A	The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(d)(2)(i)	N/A	Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(d)(2)(ii)	N/A	Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(d)(2)(iii)	N/A	If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(d)(3)	N/A	The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.520(e)	Implementation specifications: Documentation	A covered entity must document compliance with the notice requirements, as required by § 164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522	Rights to request privacy protection for protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(1)	Standard: Right of an individual to request restriction of uses and disclosures	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(1)(i)	N/A	A covered entity must permit an individual to request that the covered entity restrict:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(1)(i)(A)	N/A	Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(1)(i)(B)	N/A	Disclosures permitted under § 164.510(b).	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(1)(ii)	N/A	Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(1)(iii)	N/A	A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(1)(iv)	N/A	If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(1)(v)	N/A	A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(1)(vi)	N/A	A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(1)(vi)(A)	N/A	The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(1)(vi)(B)	N/A	The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(2)	Implementation specifications: Terminating a restriction	A covered entity may terminate a restriction, if:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(2)(i)	N/A	The individual agrees to or requests the termination in writing;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(2)(ii)	N/A	The individual orally agrees to the termination and the oral agreement is documented; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(2)(iii)	N/A	The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(2)(iii)(A)	N/A	Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(2)(iii)(B)	N/A	Only effective with respect to protected health information created or received after it has so informed the individual.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(a)(3)	Implementation specification: Documentation	A covered entity must document a restriction in accordance with § 160.530(j) of this subchapter.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(b)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(b)(1)	Standard: Confidential communications requirements	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(b)(1)(i)	N/A	A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(b)(1)(ii)	N/A	A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.522(b)(2)	Implementation specifications: Conditions on providing confidential communications	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(b)(2)(i)	N/A	A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(b)(2)(ii)	N/A	A covered entity may condition the provision of a reasonable accommodation on:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(b)(2)(ii)(A)	N/A	When appropriate, information as to how payment, if any, will be handled; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(b)(2)(ii)(B)	N/A	Specification of an alternative address or other method of contact.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(b)(2)(iii)	N/A	A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.522(b)(2)(iv)	N/A	A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.524	Access of individuals to protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.524(a)	Standard: Access to protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.524(a)(1)	Right of access	Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5)	10	
§ 164.524(a)(1)(i)	N/A	Psychotherapy notes;	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where	10	
§ 164.524(a)(1)(ii)	N/A	Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the	10	
§ 164.524(a)(1)(iii)	N/A	Protected health information maintained by a covered entity that is:	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where	10	
§ 164.524(a)(1)(iii)(A)	N/A	Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would beprohibited by law; or	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted	10	
§ 164.524(a)(1)(iii)(B)	N/A	Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where	10	
§ 164.524(a)(2)	Unreviewable grounds for denial	A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the	10	
§ 164.524(a)(2)(i)	N/A	The protected health information is excepted from the right of access by paragraph (a)(1) of this section.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where	10	
§ 164.524(a)(2)(ii)	N/A	A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5) Request correction to their PD due to inaccuracies;(6) Request erasure of their PD; and(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
§ 164.524(a)(2)(iii)	N/A	An individual's access to protected health information created or obtained by a covered health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5) Request correction to their PD due to inaccuracies;(6) Request erasure of their PD; and(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
§ 164.524(a)(2)(iv)	N/A	An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted	10	
§ 164.524(a)(2)(v)	N/A	An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the	10	
§ 164.524(a)(3)	Reviewable grounds for denial	A covered entity may deny an individual access, provided that the individual has a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted	10	
§ 164.524(a)(3)(i)	N/A	A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted	10	
§ 164.524(a)(3)(ii)	N/A	The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5)	10	
§ 164.524(a)(3)(iii)	N/A	The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5)	10	
§ 164.524(a)(4)	Review of a denial of access	If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5) Request correction to their PD due to inaccuracies;(6) Request erasure of their PD; and(7) Restrict the further collecting, receiving, processing, storing, transmitting,	10	
§ 164.524(b)	Implementation specifications: Requests for access and timely action	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.524(b)(1)	Individual's request for access	The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5)	10	
§ 164.524(b)(2)	Timely action by the covered entity	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.524(b)(2)(i)	N/A	Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the	10	
§ 164.524(b)(2)(i)(A)	N/A	If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted	10	
§ 164.524(b)(2)(i)(B)	N/A	If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the	10	
§ 164.524(b)(2)(ii)	N/A	If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the	10	
§ 164.524(b)(2)(ii)(A)	N/A	The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the	10	
§ 164.524(b)(2)(ii)(B)	N/A	The covered entity may have only one such extension of time for action on a request for access.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where	10	
§ 164.524(c)	Implementation specifications: Provision of access	If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with thefollowing requirements.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted	10	
§ 164.524(c)(1)	Providing the access requested	The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintainedin more than one designated record set or at more than one location, the covered entity need only produce the protected health information once inresponse to a request for access.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5) Request correction to their PD due to inaccuracies;(6) Request erasure of their PD; and(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
§ 164.524(c)(2)	Form of access requested	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.524(c)(2)(i)	N/A	The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.	Functional	Subset Of	Data Portability	PRI-06.6	Mechanisms exist to format exports of Personal Data (PD) in a structured, machine-readable format that allows data subjects to transfer their PD to another controller without hindrance.	10	
§ 164.524(c)(2)(ii)	N/A	Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.	Functional	Subset Of	Data Portability	PRI-06.6	Mechanisms exist to format exports of Personal Data (PD) in a structured, machine-readable format that allows data subjects to transfer their PD to another controller without hindrance.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.524(c)(2)(iii)	N/A	The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.524(c)(2)(iii)(A)	N/A	The individual agrees in advance to such a summary or explanation; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.524(c)(2)(iii)(B)	N/A	The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.524(c)(3)	Time and manner of access	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.524(c)(3)(i)	N/A	The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5) Request correction to their PD due to inaccuracies;(6) Request erasure of their PD; and(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.	10	
§ 164.524(c)(3)(ii)	N/A	If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the categories of their PD being collected, received, processed, stored and shared;(5) Request correction to their PD due to inaccuracies;(6) Request erasure of their PD; and(7) Restrict the further collecting, receiving, processing, storing, transmitting,	10	
§ 164.524(c)(4)	Fees	If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Obtain the source(s) of their PD;(4) Obtain the	10	
§ 164.524(c)(4)(i)	N/A	Labor for copying the protected health information requested by the individual, whether in paper or electronic form;	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the	10	
§ 164.524(c)(4)(ii)	N/A	Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the	10	
§ 164.524(c)(4)(iii)	N/A	Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where	10	
§ 164.524(c)(4)(iv)	N/A	Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(iii) of this section.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the	10	
§ 164.524(d)	Implementation specifications: Denial of access	If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the	10	
§ 164.524(d)(1)	Making other information accessible	The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding theprotected health information as to which the covered entity has a ground to deny access.	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;(2) Obtain answers on	10	
§ 164.524(d)(2)	Denial	The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:	Functional	Subset Of	Data Subject Empowerment	PRI-06	Mechanisms exist to provide authenticated data subjects the ability to:(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the	10	
§ 164.524(d)(2)(i)	N/A	The basis for the denial;	Functional	Subset Of	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	10	
§ 164.524(d)(2)(ii)	N/A	If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and	Functional	Subset Of	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	10	
§ 164.524(d)(2)(iii)	N/A	A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).	Functional	Subset Of	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	10	
§ 164.524(d)(3)	Other responsibility	If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.	Functional	Subset Of	Reject Unauthenticated or Untrustworthy Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthenticated, or untrustworthy, disclosure requests.	10	
§ 164.524(d)(4)	Review of denial requested	If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health careprofessional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a requestfor review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.	Functional	Subset Of	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	10	
§ 164.524(e)	Implementation specification: Documentation	A covered entity must document the following and retain the documentation as required by § 164.530(j):	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.524(e)(1)	N/A	The designated record sets that are subject to access by individuals; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.524(e)(2)	N/A	The titles of the persons or office responsible for receiving and processing requests for access by individuals.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.526	Amendment of protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.526(a)	Standard: Right to amend	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.526(a)(1)	Right to amend	An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.	Functional	Subset Of	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	10	
§ 164.526(a)(1)	Right to amend	An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.	Functional	Subset Of	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for:(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and(2) Disseminating corrections or amendments of PD to other authorized users of the PD.	10	
§ 164.526(a)(1)	Right to amend	An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.	Functional	Intersects With	Updating Personal Data (PD) Process	PRI-12	Mechanisms exist to identify and record:(1) The process(es) used to update Personal Data (PD); and(2) The frequency that such updates occur.	3	
§ 164.526(a)(2)	Denial of amendment	A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is thesubject of the request:	Functional	Subset Of	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for:(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and(2) Disseminating corrections or amendments of PD to other authorized users of the PD.	10	
§ 164.526(a)(2)(i)	N/A	Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;	Functional	Subset Of	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for:(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and(2) Disseminating corrections or amendments of PD to other authorized users of the PD.	10	
§ 164.526(a)(2)(ii)	N/A	Is not part of the designated record set;	Functional	Subset Of	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for:(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and(2) Disseminating corrections or amendments of PD to other authorized users of the PD.	10	
§ 164.526(a)(2)(iii)	N/A	Would not be available for inspection under § 164.524; or	Functional	Subset Of	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for:(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and(2) Disseminating corrections or amendments of PD to other authorized users of the PD.	10	
§ 164.526(a)(2)(iv)	N/A	Is accurate and complete.	Functional	Subset Of	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for:(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and(2) Disseminating corrections or amendments of PD to other authorized users of the PD.	10	
§ 164.526(b)	Implementation specifications: Requests for amendment and timely action	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.526(b)(1)	Individual's request for amendment	The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.	Functional	Subset Of	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	10	
§ 164.526(b)(1)	Individual's request for amendment	The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.	Functional	Subset Of	Correcting Inaccurate Personal Data (PD)	PRI-06.1	Mechanisms exist to maintain a process for:(1) Data subjects to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and(2) Disseminating corrections or amendments of PD to other authorized users of the PD.	10	
§ 164.526(b)(1)	Individual's request for amendment	The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements.	Functional	Intersects With	Updating Personal Data (PD) Process	PRI-12	Mechanisms exist to identify and record:(1) The process(es) used to update Personal Data (PD); and(2) The frequency that such updates occur.	3	
§ 164.526(b)(2)	Timely action by the covered entity	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.526(b)(2)(i)	N/A	The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits,	10	
§ 164.526(b)(2)(i)(A)	N/A	If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits,	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.526(b)(2)(i)(B)	N/A	If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(b)(2)(ii)	N/A	If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(b)(2)(ii)(A)	N/A	The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(b)(2)(ii)(B)	N/A	The covered entity may have only one such extension of time for action on a request for an amendment.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits,	10	
§ 164.526(c)	Implementation specifications: Accepting the amendment	If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.	Functional	Subset Of	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.	10	
§ 164.526(c)(1)	Making the amendment	The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.	Functional	Subset Of	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.	10	
§ 164.526(c)(2)	Informing the individual	In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.	Functional	Subset Of	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.	10	
§ 164.526(c)(3)	Informing others	The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:	Functional	Subset Of	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.	10	
§ 164.526(c)(3)(i)	N/A	Persons identified by the individual as having received protected health information about the individual and needing the amendment; and	Functional	Subset Of	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.	10	
§ 164.526(c)(3)(ii)	N/A	Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.	Functional	Subset Of	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected data subjects if their Personal Data (PD) has been corrected, amended or deleted.	10	
§ 164.526(d)	Implementation specifications: Denying the amendment	If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(d)(1)	Denial	The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(d)(1)(i)	N/A	The basis for the denial, in accordance with paragraph (a)(2) of this section;	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits,	10	
§ 164.526(d)(1)(ii)	N/A	The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits,	10	
§ 164.526(d)(1)(iii)	N/A	A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(d)(1)(iv)	N/A	A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in § 164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(d)(2)	Statement of disagreement	The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(d)(3)	Rebuttal statement	The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(d)(4)	Recordkeeping	The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(d)(5)	Future disclosures	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.526(d)(5)(i)	N/A	If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(d)(5)(ii)	N/A	If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(d)(5)(iii)	N/A	When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(e)	Implementation specification: Actions on notices of amendment	A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.	Functional	Intersects With	Updating Personal Data (PD) Process	PRI-12	Mechanisms exist to identify and record:(1) The process(es) used to update Personal Data (PD); and(2) The frequency that such updates occur.	3	
§ 164.526(e)	Implementation specification: Actions on notices of amendment	A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(f)	Implementation specification: Documentation	A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.526(f)	Implementation specification: Documentation	A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).	Functional	Intersects With	Updating Personal Data (PD) Process	PRI-12	Mechanisms exist to identify and record:(1) The process(es) used to update Personal Data (PD); and(2) The frequency that such updates occur.	3	
§ 164.528	Accounting of disclosures of protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.528(a)	Standard: Right to an accounting of disclosures of protected health information	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.528(a)(1)	N/A	An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(a)(1)(i)	N/A	To carry out treatment, payment and health care operations as provided in § 164.506;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(a)(1)(ii)	N/A	To individuals of protected health information about them as provided in § 164.502;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(a)(1)(iii)	N/A	Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(a)(1)(iv)	N/A	Pursuant to an authorization as provided in § 164.508;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(a)(1)(v)	N/A	For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(a)(1)(vi)	N/A	For national security or intelligence purposes as provided in § 164.512(k)(2);	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(a)(1)(vii)	N/A	To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(a)(1)(viii)	N/A	As part of a limited data set in accordance with § 164.514(e); or	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(a)(1)(ix)	N/A	That occurred prior to the compliance date for the covered entity.	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(a)(2)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.528(a)(2)(i)	N/A	The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.528(a)(2)(ii)	N/A	If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.528(a)(2)(ii)(A)	N/A	Document the statement, including the identity of the agency or official making the statement;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.528(a)(2)(ii)(B)	N/A	Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.528(a)(2)(ii)(C)	N/A	Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.528(a)(3)	N/A	An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.528(b)	Implementation specifications: Content of the accounting	The covered entity must provide the individual with a written accounting that meets the following requirements.	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(1)	N/A	Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(2)	N/A	Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(2)(i)	N/A	The date of the disclosure;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(2)(ii)	N/A	The name of the entity or person who received the protected health information and, if known, the address of such entity or person;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(2)(iii)	N/A	A brief description of the protected health information disclosed; and	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(2)(iv)	N/A	A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §§ 164.502(a)(2)(ii) or 164.512, if any.	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(3)	N/A	If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under §§ 164.502(a)(2)(ii) or 164.512, the accounting may, with respect to such multiple disclosures, provide:	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(3)(i)	N/A	The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(3)(ii)	N/A	The frequency, periodicity, or number of the disclosures made during the accounting period; and	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(3)(iii)	N/A	The date of the last such disclosure during the accounting period.	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(4)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.528(b)(4)(i)	N/A	If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with § 164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(4)(i)(A)	N/A	The name of the protocol or other research activity;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(4)(i)(B)	N/A	A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(4)(i)(C)	N/A	A brief description of the type of protected health information that was disclosed;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(4)(i)(D)	N/A	The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(4)(i)(E)	N/A	The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(4)(i)(F)	N/A	A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(b)(4)(ii)	N/A	If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(c)	Implementation specifications: Provision of the accounting	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.528(c)(1)	N/A	The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(c)(1)(i)	N/A	The covered entity must provide the individual with the accounting requested; or	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(c)(1)(ii)	N/A	If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(c)(1)(ii)(A)	N/A	The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(c)(1)(ii)(B)	N/A	The covered entity may have only one such extension of time for action on a request for an accounting.	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(c)(2)	N/A	The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(d)	Implementation specification: Documentation	A covered entity must document the following and retain the documentation as required by § 164.530(j):	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(d)(1)	N/A	The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(d)(2)	N/A	The written accounting that is provided to the individual under this section; and	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.528(d)(3)	N/A	The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.	Functional	Subset Of	Accounting of Disclosures	PRI-14.1	Mechanisms exist to provide data subjects with an accounting of disclosures of their Personal Data (PD) controlled by:(1) The organization; and/or(2) Relevant third-parties that their PD was shared with.	10	
§ 164.530	Administrative requirements	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(a)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(a)(1)	Standard: Personnel designations	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(a)(1)(i)	N/A	A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
§ 164.530(a)(1)(i)	N/A	A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.	Functional	Subset Of	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	10	
§ 164.530(a)(1)(ii)	N/A	A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.	Functional	Subset Of	Data Protection Officer (DPO)	PRI-01.4	Mechanisms exist to appoint a Data Protection Officer (DPO):(1) Based on professional qualifications; and(2) To be involved in all issues related to how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed.	10	
§ 164.530(a)(2)	Implementation specification: Personnel designations	A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.	Functional	Equal	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	10	
§ 164.530(a)(2)	Implementation specification: Personnel designations	A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
§ 164.530(b)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.530(b)(1)	Standard: Training	A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.	Functional	Subset Of	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	10	
§ 164.530(b)(1)	Standard: Training	A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.	Functional	Subset Of	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training:(1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and(3) Annually thereafter.	10	
§ 164.530(b)(2)	Implementation specifications: Training	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(b)(2)(i)	N/A	A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for	10	
§ 164.530(b)(2)(i)(A)	N/A	To each member of the covered entity's workforce by no later than the compliance date for the covered entity;	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for	10	
§ 164.530(b)(2)(i)(B)	N/A	Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
§ 164.530(b)(2)(i)(C)	N/A	To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
§ 164.530(b)(2)(ii)	N/A	A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
§ 164.530(c)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(c)(1)	Standard: Safeguards	A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
§ 164.530(c)(2)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(c)(2)(i)	Implementation specification: Safeguards	A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
§ 164.530(c)(2)(i)	Implementation specification: Safeguards	A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.	Functional	Subset Of	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	10	
§ 164.530(c)(2)(ii)	N/A	A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
§ 164.530(c)(2)(ii)	N/A	A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8	
§ 164.530(d)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(d)(1)	Standard: Complaints to the covered entity	A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.530(d)(2)	Implementation specification: Documentation of complaints	As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.	Functional	Subset Of	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
§ 164.530(e)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(e)(1)	Standard: Sanctions	A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.	Functional	Subset Of	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	10	
§ 164.530(e)(2)	Implementation specification: Documentation	As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
§ 164.530(f)	Standard: Mitigation	A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
§ 164.530(g)	Standard: Refraining from intimidating or retaliatory acts	A covered entity—	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(g)(1)	N/A	May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D of this part, including the filing of a complaint under this section; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(g)(2)	N/A	Must refrain from intimidation and retaliation as provided in § 160.316 of this subchapter.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(h)	Standard: Waiver of rights	A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(i)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(i)(1)	Standard: Policies and procedures	A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
§ 164.530(i)(1)	Standard: Policies and procedures	A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
§ 164.530(i)(1)	Standard: Policies and procedures	A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
§ 164.530(i)(2)	Standard: Changes to policies and procedures	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(i)(2)(i)	N/A	A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart or subpart D of this part.	Functional	Subset Of	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
§ 164.530(i)(2)(ii)	N/A	When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or	Functional	Subset Of	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
§ 164.530(i)(2)(iii)	N/A	A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.	Functional	Subset Of	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
§ 164.530(i)(3)	Implementation specification: Changes in law	Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.	Functional	Subset Of	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
§ 164.530(i)(4)	Implementation specifications: Changes to privacy practices stated in the notice	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.530(i)(4)(i)	N/A	To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(i)(4)(i)(A)	N/A	Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
§ 164.530(i)(4)(i)(B)	N/A	Document the policy or procedure, as revised, as required by paragraph (j) of this section; and	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are	10	
§ 164.530(i)(4)(i)(C)	N/A	Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.	Functional	Subset Of	Data Privacy Notice	PRI-02	Mechanisms exist to:(1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary;(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;(5) Periodically, review and update the content of the privacy notice, as necessary; and(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	10	
§ 164.530(i)(4)(ii)	N/A	If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.530(i)(4)(ii)(A)	N/A	Such change meets the implementation specifications in paragraphs (i)(4)(ii)(A)-(C) of this section; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(i)(4)(ii)(B)	N/A	Such change is effective only with respect to protected health information created or received after the effective date of the notice.	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the	10	
§ 164.530(i)(5)	Implementation specification: Changes to other policies or procedures	A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
§ 164.530(i)(5)(i)	N/A	The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
§ 164.530(i)(5)(ii)	N/A	Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
§ 164.530(j)	N/A	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(j)(1)	Standard: Documentation	A covered entity must:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(j)(1)(i)	N/A	Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
§ 164.530(j)(1)(ii)	N/A	If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(j)(1)(iii)	N/A	If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(j)(1)(iv)	N/A	Maintain documentation sufficient to meet its burden of proof under § 164.414(b).	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(j)(2)	Implementation specification: Retention period	A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.	Functional	Subset Of	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	
§ 164.530(k)	Standard: Group health plans	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(k)(1)	N/A	A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(k)(1)(i)	N/A	The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(k)(1)(ii)	N/A	The group health plan does not create or receive protected health information, except for:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(k)(1)(ii)(A)	N/A	Summary health information as defined in § 164.504(a); or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(k)(1)(ii)(B)	N/A	Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.530(k)(2)	N/A	A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532	Transition provisions	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(a)	Standard: Effect of prior authorizations	Notwithstanding §§ 164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, a waiver of informed consent by an IRB, or a waiver of authorization in accordance with § 164.512(i)(1)(i).	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.532(a)	Standard: Effect of prior authorizations	Notwithstanding §§ 164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, a waiver of informed consent by an IRB, or a waiver of authorization in accordance with § 164.512(i)(1)(i).	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.532(b)	Implementation specification: Effect of prior authorization for purposes other than research	Notwithstanding any provisions in § 164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with § 164.522(a).	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.532(b)	Implementation specification: Effect of prior authorization for purposes other than research	Notwithstanding any provisions in § 164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with § 164.522(a).	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.532(c)	Implementation specification: Effect of prior permission for research	Notwithstanding any provisions in §§ 164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with § 164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.532(c)	Implementation specification: Effect of prior permission for research	Notwithstanding any provisions in §§ 164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with § 164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:	Functional	Subset Of	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to:(1) The purpose(s) originally collected, consistent with the data privacy notice(s);(2) What is authorized by the data subject, or authorized agent; and(3) What is consistent with applicable laws, regulations and contractual obligations.	10	
§ 164.532(c)(1)	N/A	An authorization or other express legal permission from an individual to use or disclose protected health information for the research;	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.532(c)(2)	N/A	The informed consent of the individual to participate in the research;	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(c)(3)	N/A	A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with § 164.508 if, after the compliance date, informed consent is sought from an individual participating in the research; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(c)(4)	N/A	A waiver of authorization in accordance with § 164.512(i)(1)(i).	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(d)	Standard: Effect of prior contracts or other arrangements with business associates	Notwithstanding any other provisions of this part, a covered entity, or business associate with respect to a subcontractor, may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), only in accordance with paragraph (e) of this section.	Functional	Subset Of	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	10	
§ 164.532(e)	Implementation specification: Deemed compliance	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
§ 164.532(e)(1)	Qualification	Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(e)(1)(i)	N/A	Prior to January 25, 2013, such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of §§ 164.314(a) or 164.504(e) that were in effect on such date; and	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(e)(1)(ii)	N/A	The contract or other arrangement is not renewed or modified from March 26, 2013, until September 23, 2013.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(e)(2)	Limited deemed compliance period	A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section shall be deemed compliant until the earlier of:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(e)(2)(i)	N/A	The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(e)(2)(ii)	N/A	September 22, 2014.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(e)(3)	Covered entity responsibilities	Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and §§ 164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(f)	Effect of prior data use agreements	If, prior to January 25, 2013, a covered entity has entered into and is operating pursuant to a data use agreement with a recipient of a limited data set that complies with § 164.514(e), notwithstanding § 164.502(a)(5)(ii), the covered entity may continue to disclose a limited data set pursuant to such agreement in exchange for remuneration from or on behalf of the recipient of the protected health information until the earlier of:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(f)(1)	N/A	The date such agreement is renewed or modified on or after September 23, 2013; or	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.532(f)(2)	N/A	September 22, 2014.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.534	Compliance dates for initial implementation of the privacy standards	[no content]	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.534(a)	Health care providers	A covered health care provider must comply with the applicable requirements of this subpart no later than April 14, 2003.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.534(b)	Health plans	A health plan must comply with the applicable requirements of this subpart no later than the following as applicable:	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.534(b)(1)	Health plans other han small health plans	14-Apr-03	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.534(b)(2)	Small health plans	April 14, 2004.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	
§ 164.534(c)	Health clearinghouses	A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 14, 2003.	Functional	No Relationship	N/A	N/A	No applicable SCF control	0	