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: **HHS § 155.260 - Privacy and Security of Personally Identifiable Information (2016)**
Focal Document URL: https://www.govinfo.gov/content/pkg/CFR-2016-title45-vol1/pdf/CFR-2016-title45-vol1-sec155-260.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-hhs-45-cfr-155-260-2016.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	Notes
155.260	Privacy and security of personally identifiable information.	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(a)	Creation, collection, use and disclosure.	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(a)(1)	N/A	Where the Exchange creates or collects personally identifiable information for the purposes of determining eligibility for enrollment in a qualified health plan; determining eligibility for other insurance affordability programs, as defined in §155.300; or determining eligibility for exemptions from the individual shared responsibility provisions in section 5000A of the Code, the Exchange may only use or disclose such personally identifiable information to the extent such information is necessary:	Functional	Intersects With	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
155.260(a)(1)(i)	N/A	For the Exchange to carry out the functions described in §155.200;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(a)(1)(ii)	N/A	For the Exchange to carry out other functions not described in paragraph (a)(1)(i) of this section, which the Secretary determines to be in compliance with section 1411(g)(2)(A) of the Affordable Care Act and for which an individual provides consent for his or her information to be used or disclosed; or	Functional	Intersects With	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
155.260(a)(1)(iii)	N/A	For the Exchange to carry out other functions not described in paragraphs (a)(1)(i) and (ii) of this section, for which an individual provides consent for his or her information to be used or disclosed, and which the Secretary determines are in compliance with section 1411(g)(2)(A) of the Affordable Care Act under the following substantive and procedural requirements:	Functional	Intersects With	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
155.260(a)(1)(iii)(A)	Substantive requirements.	The Secretary may approve other uses and disclosures of personally identifiable information created or collected as described in paragraph (a)(1) of this section that are not described in paragraphs (a)(1)(i) or (ii) of this section, provided that HHS determines that the information will be used only for the purposes of and to the extent necessary in ensuring the efficient operation of the Exchange consistent with section 1411(g)(2)(A) of the Affordable Care Act, and that the uses and disclosures are also permissible under relevant law and policy.	Functional	Intersects With	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	5	
155.260(a)(1)(iii)(B)	Procedural requirements for approval of a use or disclosure of personally identifiable information.	To seek approval for a use or disclosure of personally identifiable information created or collected as described in paragraph (a)(1) of this section that is not described in paragraphs (a)(1)(i) or (ii) of this section, the Exchange must submit the following information to HHS:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(a)(1)(iii)(B)(1)	N/A	Identity of the Exchange and appropriate contact persons;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(a)(1)(iii)(B)(2)	N/A	Detailed description of the proposed use or disclosure, which must include, but not necessarily be limited to, a listing or description of the specific information to be used or disclosed and an identification of the persons or entities that may access or receive the information;	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(a)(1)(iii)(B)(3)	N/A	Description of how the use or disclosure will ensure the efficient operation of the Exchange consistent with section 1411(g)(2)(A) of the Affordable Care Act; and	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(a)(1)(iii)(B)(4)	N/A	Description of how the information to be used or disclosed will be protected in compliance with privacy and security standards that meet the requirements of this section or other relevant law, as applicable.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(a)(2)	N/A	The Exchange may not create, collect, use, or disclose personally identifiable information unless the creation, collection, use, or disclosure is consistent with this section.	Functional	Subset Of	Limitations on Use	DCH-10.1	Mechanisms exist to restrict the use and distribution of sensitive/regulated data.	10	
155.260(a)(3)	N/A	The Exchange must establish and implement privacy and security standards that are consistent with the following principles:	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
155.260(a)(3)	N/A	The Exchange must establish and implement privacy and security standards that are consistent with the following principles:	Functional	Intersects With	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.	8	
155.260(a)(3)(i)	Individual access.	Individuals should be provided with a simple and timely means to access and obtain their personally identifiable information in a readable form and format;	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	
155.260(a)(3)(ii)	Correction.	Individuals should be provided with a timely means to dispute the accuracy or integrity of their personally identifiable information and to have erroneous information corrected or to have a dispute documented if their requests are denied;	Functional	Intersects With	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to maintain a process for data subjects to appeal an adverse decision.	8	
155.260(a)(3)(iii)	Openness and transparency.	There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information;	Functional	Intersects With	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.	8	
155.260(a)(3)(iv)	Individual choice.	Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their personally identifiable 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	
155.260(a)(3)(v)	Collection, use, and disclosure limitations.	Personally identifiable information should be created, collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately;	Functional	Intersects With	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.	8	
155.260(a)(3)(vi)	Data quality and integrity.	Persons and entities should take reasonable steps to ensure that personally identifiable information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner;	Functional	Intersects With	Personal Data (PD) Accuracy & Integrity	PRI-05.2	Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by:(1) Keeping PD up-to-date; and(2) Remediating identified inaccuracies, as necessary.	5	
155.260(a)(3)(vi)	Data quality and integrity.	Persons and entities should take reasonable steps to ensure that personally identifiable information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner;	Functional	Intersects With	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.	5	
155.260(a)(3)(vi)	Data quality and integrity.	Persons and entities should take reasonable steps to ensure that personally identifiable information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner;	Functional	Intersects With	Personal Data (PD) Accuracy & Integrity	PRI-05.2	Mechanisms exist to ensure the accuracy and relevance of Personal Data (PD) throughout the information lifecycle by:(1) Keeping PD up-to-date; and(2) Remediating identified inaccuracies, as necessary.	5	
155.260(a)(3)(vii)	Safeguards.	Personally identifiable information should be protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure; and,	Functional	Subset Of	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	10	
155.260(a)(3)(viii)	Accountability.	These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.	Functional	Intersects With	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.	8	
155.260(a)(3)(viii)	Accountability.	These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.	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	
155.260(a)(3)(viii)	Accountability.	These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
155.260(a)(4)	N/A	For the purposes of implementing the principle described in paragraph (a)(3)(vii) of this section, the Exchange must establish and implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws (including this section) to ensure—	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
155.260(a)(4)	N/A	For the purposes of implementing the principle described in paragraph (a)(3)(vii) of this section, the Exchange must establish and implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws (including this section) to ensure—	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	
155.260(a)(4)	N/A	For the purposes of implementing the principle described in paragraph (a)(3)(vii) of this section, the Exchange must establish and implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws (including this section) to ensure—	Functional	Intersects With	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.	3	
155.260(a)(4)	N/A	For the purposes of implementing the principle described in paragraph (a)(3)(vii) of this section, the Exchange must establish and implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws (including this section) to ensure—	Functional	Intersects With	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.	3	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
155.260(a)(4)	N/A	For the purposes of implementing the principle described in paragraph (a)(3)(vii) of this section, the Exchange must establish and implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws (including this section) to ensure—	Functional	Intersects With	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.	3	
155.260(a)(4)	N/A	For the purposes of implementing the principle described in paragraph (a)(3)(vii) of this section, the Exchange must establish and implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws (including this section) to ensure—	Functional	Intersects With	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.	3	
155.260(a)(4)(i)	N/A	The confidentiality, integrity, and availability of personally identifiable information created, collected, used, and/or disclosed by the Exchange;	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	
155.260(a)(4)(ii)	N/A	Personally identifiable information is only used by or disclosed to those authorized to receive or view it;	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	8	
155.260(a)(4)(ii)	N/A	Personally identifiable information is only used by or disclosed to those authorized to receive or view it;	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	8	
155.260(a)(4)(ii)	N/A	Personally identifiable information is only used by or disclosed to those authorized to receive or view it;	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	
155.260(a)(4)(iii)	N/A	Return information, as such term is defined by section 6103(b)(2) of the Code, is kept confidential under section 6103 of the Code;	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	
155.260(a)(4)(iv)	N/A	Personally identifiable information is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information;	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
155.260(a)(4)(v)	N/A	Personally identifiable information is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law; and	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
155.260(a)(4)(vi)	N/A	Personally identifiable information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules;	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	8	
155.260(a)(4)(vi)	N/A	Personally identifiable information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules;	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.	8	
155.260(a)(4)(vi)	N/A	Personally identifiable information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules;	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	8	
155.260(a)(5)	N/A	The Exchange must monitor, periodically assess, and update the security controls and related system risks to ensure the continued effectiveness of those controls.	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	
155.260(a)(6)	N/A	The Exchange must develop and utilize secure electronic interfaces when sharing personally identifiable information electronically.	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.	8	
155.260(a)(6)	N/A	The Exchange must develop and utilize secure electronic interfaces when sharing personally identifiable information electronically.	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	8	
155.260(a)(6)	N/A	The Exchange must develop and utilize secure electronic interfaces when sharing personally identifiable information electronically.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
155.260(b)	Application to non-Exchange entities—	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(b)(1)	Non-Exchange entities.	A nonExchange entity is any individual or entity that:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(b)(1)(i)	N/A	Gains access to personally identifiable information submitted to an Exchange; or	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(b)(1)(ii)	N/A	Collects, uses, or discloses personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing functions agreed to with the Exchange.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(b)(2)	N/A	Prior to any person or entity becoming a non-Exchange entity, Exchanges must execute with the person or entity a contract or agreement that includes:	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	
155.260(b)(2)(i)	N/A	A description of the functions to be performed by the non-Exchange 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	
155.260(b)(2)(ii)	N/A	A provision(s) binding the nonExchange entity to comply with the privacy and security standards and obligations adopted in accordance with paragraph (b)(3) of this section, and specifically listing or incorporating those privacy and security standards and obligations;	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	
155.260(b)(2)(iii)	N/A	A provision requiring the nonExchange entity to monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls in accordance with paragraph (a)(5) 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	
155.260(b)(2)(iv)	N/A	A provision requiring the non-Exchange entity to inform the Exchange of any change in its administrative, technical, or operational environments defined as material within the contract; 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	
155.260(b)(2)(v)	N/A	A provision that requires the nonExchange entity to bind any downstream entities to the same privacy and security standards and obligations to which the non-Exchange entity has agreed in its contract or agreement with the Exchange.	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	
155.260(b)(3)	N/A	When collection, use or disclosure is not otherwise required by law, the privacy and security standards to which an Exchange binds non-Exchange entities must:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(b)(3)(i)	N/A	Be consistent with the principles and requirements listed in paragraphs (a)(1) through (6) of this section, including being at least as protective as the standards the Exchange has established and implemented for itself in compliance with paragraph (a)(3) of this section;	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
155.260(b)(3)(ii)	N/A	Comply with the requirements of paragraphs (c), (d), (f), and (g) of this section; and	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
155.260(b)(3)(iii)	N/A	Take into specific consideration:	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
155.260(b)(3)(iii)(A)	N/A	The environment in which the non-Exchange entity is operating;	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
155.260(b)(3)(iii)(B)	N/A	Whether the standards are relevant and applicable to the non-Exchange entity's duties and activities in connection with the Exchange; and	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
155.260(b)(3)(iii)(C)	N/A	Any existing legal requirements to which the non-Exchange entity is bound in relation to its administrative, technical, and operational controls and practices, including but not limited to, its existing data handling and information technology processes and protocols.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
155.260(c)	Workforce compliance.	The Exchange must ensure its workforce complies with the policies and procedures developed and implemented by the Exchange to comply with this section.	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	
155.260(c)	Workforce compliance.	The Exchange must ensure its workforce complies with the policies and procedures developed and implemented by the Exchange to comply with this section.	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.	8	
155.260(d)	Written policies and procedures.	Policies and procedures regarding the creation collection, use, and disclosure of personally identifiable information must, at minimum:	Functional	Intersects With	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.	5	
155.260(d)	Written policies and procedures.	Policies and procedures regarding the creation collection, use, and disclosure of personally identifiable information must, at minimum:	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	
155.260(d)(1)	N/A	Be in writing, and available to the Secretary of HHS upon request; 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	
155.260(d)(2)	N/A	Identify applicable law governing collection, use, and disclosure of personally identifiable 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	
155.260(e)	Data sharing.	Data matching and sharing arrangements that facilitate the sharing of personally identifiable information between the Exchange and agencies administering Medicaid, CHIP or the BHP for the exchange of eligibility information must:	Functional	Intersects With	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.	5	
155.260(e)(1)	N/A	Meet any applicable requirements described in this section;	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
155.260(e)(2)	N/A	Meet any applicable requirements described in section 1413(c)(1) and (c)(2) of the Affordable Care Act;	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
155.260(e)(3)	N/A	Be equal to or more stringent than the requirements for Medicaid programs under section 1942 of the Act; and	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
155.260(e)(4)	N/A	For those matching agreements that meet the definition of ''matching program'' under 5 U.S.C. 552a(a)(8), comply with 5 U.S.C. 552a(o).	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
155.260(f)	Compliance with the Code.	Return information, as defined in section 6103(b)(2) of the Code, must be kept confidential and disclosed, used, and maintained only in accordance with section 6103 of the Code.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
155.260(g)	Improper use and disclosure of information.	Any person who knowingly and willfully uses or discloses information in violation of section 1411(g) of the Affordable Care Act will be subject to a CMP of not more than $25,000 as adjusted annually under 45 CFR part 102 per person or entity, per use or disclosure, consistent with the bases and process for imposing civil penalties specified at §155.285, in addition to other penalties that may be prescribed by law.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control