

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: <https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/>

Focal Document: Illinois Personal Information Protection Act (PIPA) (2006)
Focal Document URL: <https://www.ilga.gov/Legislation/ILCS/Articles/Articles7.htm?ActID=2702&ChapterID=67>
Published STRM URL: <https://content.securecontrolsframework.com/strm/scf-strm-usa-state-il-pipa-2006.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
1	Short title	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5	Definitions	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10	Notice of breach; notice to Attorney General	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10(a)	Notice of breach; notice to Attorney General	Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows: The notification shall not, however, include information concerning the number of Illinois residents affected by the 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	
10(a)(1)	Notice of breach; notice to Attorney General	With respect to personal information as defined in Section 5 in paragraph (1) of the definition of "personal information":	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	
10(a)(1)(A)	Notice of breach; notice to Attorney General	the toll-free numbers and addresses for consumer reporting agencies;	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	
10(a)(1)(B)	Notice of breach; notice to Attorney General	the toll-free number, address, and website address for the Federal Trade Commission; and	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	
10(a)(1)(C)	Notice of breach; notice to Attorney General	a statement that the individual can obtain information from these sources about fraud alerts and security freezes.	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	
10(a)(2)	Notice of breach; notice to Attorney General	With respect to personal information defined in Section 5 in paragraph (2) of the definition of "personal information", notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.	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	
10(b)	Notice of breach; notice to Attorney General	Any data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the 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	
10(b-5)	Notice of breach; notice to Attorney General	The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification no longer interferes with the investigation.	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	
10(c)	Notice of breach; notice to Attorney General	For purposes of this Section, notice to consumers may be provided by one of the following methods:	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	
10(c)(1)	Notice of breach; notice to Attorney General	written notice;	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	
10(c)(2)	Notice of breach; notice to Attorney General	electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7003 of Title 15 of the Illinois Code; or	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	
10(c)(3)	Notice of breach; notice to Attorney General	substitute notice, if the data collector demonstrates that the cost of providing notice would exceed \$250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media or, if the breach impacts residents in one geographic area, to prominent local media in areas where affected individuals are likely to reside if such notice is reasonably calculated to give actual notice to persons whom notice is required.	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	
10(d)	Notice of breach; notice to Attorney General	Notwithstanding any other subsection in this Section, a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.	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	
10(e)(1)	Notice of breach; notice to Attorney General	This subsection does not apply to data collectors that are covered entities or business associates and are in compliance with Section 50.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10(e)(2)	Notice of breach; notice to Attorney General	Any data collector required to issue notice pursuant to this Section to more than 500 Illinois residents as a result of a single breach of the security system shall provide notice to the Attorney General of the breach, including: Such notification must be made in the most expedient time possible and without unreasonable delay but in no event later than when the data collector provides notice to consumers pursuant to this Section. If the date of the breach is unknown at the time the notice is sent to the Attorney General, the data collector shall send the Attorney General the date of the breach as soon as possible. Upon receiving notification from a data collector of a breach of personal information, the Attorney General may publish the name of the data collector that suffered the breach, the types of personal information compromised in the breach, and the date range of the breach.(Source: P.A. 100-201, eff. 8-18-17; 101-343, eff. 1-1-20.)	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	
10(e)(2)(A)	Notice of breach; notice to Attorney General	A description of the nature of the breach of security or unauthorized acquisition or use.	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	
10(e)(2)(B)	Notice of breach; notice to Attorney General	The number of Illinois residents affected by such incident at the time of notification.	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	
10(e)(2)(C)	Notice of breach; notice to Attorney General	Any steps the data collector has taken or plans to take relating to the incident.	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	
12	Notice of breach; State agency	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12(a)	Notice of breach; State agency	Any State agency that collects personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data or written material following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows: The notification shall not, however, include information concerning the number of Illinois residents affected by the 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	
12(a)(1)	Notice of breach; State agency	With respect to personal information defined in Section 5 in paragraph (1) of the definition of "personal information":	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	
12(a)(1)(i)	Notice of breach; State agency	the toll-free numbers and addresses for consumer reporting agencies;	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	
12(a)(1)(ii)	Notice of breach; State agency	the toll-free number, address, and website address for the Federal Trade Commission; and	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	
12(a)(1)(iii)	Notice of breach; State agency	a statement that the individual can obtain information from these sources about fraud alerts and security freezes.	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	

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
12(a)(2)	Notice of breach: State agency	With respect to personal information as defined in Section 5 in paragraph (2) of the definition of "personal information," notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.	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	
12(a)(5)	Notice of breach: State agency	The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the State agency with the delay. However, the State agency must notify the Illinois resident as soon as notification will no longer interfere with the investigation.	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	
12(b)	Notice of breach: State agency	For purposes of this Section, notice to residents may be provided by one of the following methods:	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	
12(b)(1)	Notice of breach: State agency	written notice;	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	
12(b)(2)	Notice of breach: State agency	electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or	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	
12(b)(3)	Notice of breach: State agency	substitute notice, if the State agency demonstrates that the cost of providing notice will exceed \$250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the State agency does not have sufficient contact information. Substitute notice shall consist of all of the following:	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	
12(b)(3)(i)	Notice of breach: State agency	(i) email notice if the State agency has an email address for the subject persons;	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	
12(b)(3)(ii)	Notice of breach: State agency	(ii) conspicuous posting of the notice on the State agency's web site page if the State agency maintains one; and	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	
12(b)(3)(iii)	Notice of breach: State agency	(iii) notification to major statewide media.	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	
12(c)	Notice of breach: State agency	Notwithstanding subsection (b), a State agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act shall be deemed in compliance with the notification requirements of this Section if the State agency notifies subject persons in accordance with its policies in the event of a breach of the security of the system data or written material.	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	
12(d)	Notice of breach: State agency	If a State agency is required to notify more than 1,000 persons of a breach of security pursuant to this Section, the State agency shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. Section 1681(a), of the timing, distribution, and content of the notices. Nothing in this subsection (d) shall be construed to require the State agency to provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients.	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	
12(e)	Notice of breach: State agency	Notice to Attorney General. Any State agency that suffers a single breach of the security of the data concerning the personal information of more than 250 Illinois residents shall provide notice to the Attorney General of the breach, including: Such notification must be made within 45 days of the State agency's discovery of the security breach or when the State agency provides any notice to consumers required by this Section, whichever is sooner, unless the State agency has good cause for reasonable delay to determine the scope of the breach and restore the integrity, security, and confidentiality of the data system, or when law enforcement requests in writing to withhold disclosure of some or all of the information required in the notification under this Section. If the date or timeframe of the breach is unknown at the time the notice is sent to the Attorney General, the State agency shall send the Attorney General the date or timeframe of the breach as soon as possible.	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	
12(e)(A)	Notice of breach: State agency	The types of personal information compromised in the 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	
12(e)(B)	Notice of breach: State agency	The number of Illinois residents affected by such incident at the time of notification.	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	
12(e)(C)	Notice of breach: State agency	Any steps the State agency has taken or plans to take relating to notification of the breach to consumers.	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	
12(e)(D)	Notice of breach: State agency	The date and timeframe of the breach, if known at the time notification is provided.	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	
12(f)	Notice of breach: State agency	In addition to the report required by Section 25 of this Act, if the State agency that suffers a breach determines the identity of the actor who perpetrated the breach, then the State agency shall report this information, within 5 days after the determination, to the General Assembly, provided that such report would not jeopardize the security of Illinois residents or compromise a security investigation.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5	
12(g)	Notice of breach: State agency	A State agency directly responsible to the Governor that has been subject to or has reason to believe it has been subject to a single breach of the security of the data concerning the personal information of more than 250 Illinois residents or an instance of aggravated computer tampering, as defined in Section 17-53 of the Criminal Code of 2012, shall notify the Office of the Chief Information Security Officer of the Illinois Department of Innovation and Technology and the Attorney General regarding the breach or instance of aggravated computer tampering. The notification shall be made without delay, but no later than 72 hours following the discovery of the incident. Upon receiving notification of such incident, the Chief Information Security Officer shall without delay take necessary and reasonable actions to: The Department of Innovation and Technology may agree to submit the reports required in subsections (e) and (f) of this Section and in Section 25 in lieu of the impacted agency.	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	
12(g)(ii)	Notice of breach: State agency	assess the incident to determine the potential impact on the overall confidentiality, security, and availability of State of Illinois data and information systems;	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	
12(g)(iii)	Notice of breach: State agency	ensure the security incident is contained to minimize additional impact and risk to the State;	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	
12(g)(iii)	Notice of breach: State agency	identify the root cause of the incident;	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	
12(g)(iv)	Notice of breach: State agency	provide recommendations to the impacted State agency to assist with eradicating the threat and removing and mitigating any vulnerabilities to reduce the risk of further compromise; and	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	
12(g)(v)	Notice of breach: State agency	assist the impacted State agency in any necessary recovery efforts to ensure effective return to a state of normal operations.	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	
12(h)	Notice of breach: State agency	Upon receiving notification from a State agency of a breach of personal information or from the Department of Innovation and Technology in lieu of the impacted agency, the Attorney General may publish the name of the State agency that suffered the breach, the types of personal information compromised in the breach, and the date range of the breach.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
15	Waiver	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
20	Violation	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
25	Annual reporting	Any State agency that collects personal data and has had a breach of security of the system data or written material shall submit a report within 5 business days of the discovery or notification of the breach to the General Assembly, listing the breaches and outlining any corrective measures that have been taken to prevent future breaches of the security of the system data or written material. Any State agency that has submitted a report under this Section shall submit an annual report listing all breaches of security of the system data or written materials and the corrective measures that have been taken to prevent future breaches.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5	
30	Safe disposal of information	Any State agency that collects personal data that is no longer needed or stored at the agency shall dispose of the personal data or written material it has collected in such a manner as to ensure the security and confidentiality of the material.	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	
40	Disposal of materials containing personal information; Attorney General	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
40(a)	Disposal of materials containing personal information; Attorney General	In this Section, "person" means: a natural person, a corporation, partnership, association, or other legal entity; a unit of local government or any agency, department, division, bureau, board, commission, or committee thereof; or the State of Illinois or any constitutional officer, agency, department, division, bureau, board, commission, or committee thereof.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

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
40(b)	Disposal of materials containing personal information; Attorney General	A person must dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable. Proper disposal methods include, but are not limited to, the following:	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
40(b)(1)	Disposal of materials containing personal information; Attorney General	Paper documents containing personal information may be either redacted, burned, pulverized, or shredded so that personal information cannot practically be read or reconstructed.	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
40(b)(2)	Disposal of materials containing personal information; Attorney General	Electronic media and other non-paper media containing personal information may be destroyed or erased so that personal information cannot practically be read or reconstructed.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
40(c)	Disposal of materials containing personal information; Attorney General	Any person disposing of materials containing personal information may contract with a third party to dispose of such materials in accordance with this Section. Any third party that contracts with a person to dispose of materials containing personal information must implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation, and disposal of materials containing personal information.	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
40(d)	Disposal of materials containing personal information; Attorney General	Any person, including but not limited to a third party referenced in subsection (c), who violates this Section is subject to a civil penalty of not more than \$100 for each individual with respect to whom personal information is disposed of in violation of this Section. A civil penalty may not, however, exceed \$50,000 for each instance of improper disposal of materials containing personal information. The Attorney General may impose a civil penalty after notice to the person accused of violating this Section and an opportunity for that person to be heard in the matter. The Attorney General may file a civil action in the circuit court to recover any penalty imposed under this Section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
40(e)	Disposal of materials containing personal information; Attorney General	In addition to the authority to impose a civil penalty under subsection (d), the Attorney General may bring an action in the circuit court to remedy a violation of this Section, seeking any appropriate relief.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
40(f)	Disposal of materials containing personal information; Attorney General	A financial institution under 15 U.S.C. 6801 et. seq. or any person subject to 15 U.S.C. 1681w is exempt from this Section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
45	Data security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
45(a)	Data security	A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.	Functional	Intersects With	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.	8	
45(a)	Data security	A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	8	
45(b)	Data security	A contract for the disclosure of personal information concerning an Illinois resident that is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.	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.	8	
45(b)	Data security	A contract for the disclosure of personal information concerning an Illinois resident that is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.	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.	8	
45(c)	Data security	If a state or federal law requires a data collector to provide greater protection to records that contain personal information concerning an Illinois resident that are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this Section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
45(d)	Data security	A data collector that is subject to and in compliance with the standards established pursuant to Section 501(b) of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801, shall be deemed to be in compliance with the provisions of this Section.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
50	Entities subject to the federal Health Insurance Portability and Accountability Act of 1996	Any covered entity or business associate that is subject to and in compliance with the privacy and security standards for the protection of electronic health information established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act shall be deemed to be in compliance with the provisions of this Act, provided that any covered entity or business associate required to provide notification of a breach to the Secretary of Health and Human Services pursuant to the Health Information Technology for Economic and Clinical Health Act also provides such notification to the Attorney General within 5 business days of notifying the Secretary.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control