HITRUST Common Security Framework Summary of Changes

DRAFT Privacy Controls

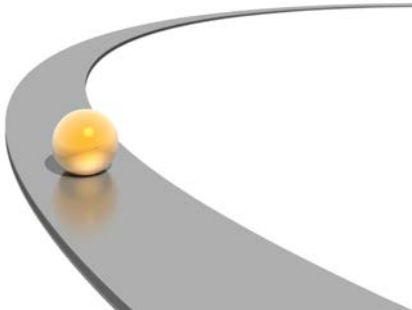
Incorporates privacy changes in NIST SP 800-53 r4.

Fundamental to HITRUST's mission is the availability of a Common Security Framework (CSF) that provides the needed structure, clarity, functionality and cross-references to authoritative sources. The initial development of the CSF leveraged nationally and internationally accepted standards including ISO, NIST, PCI, HIPAA, and COBIT to ensure a comprehensive set of baseline security controls. The CSF normalizes these security requirements and provides clarity and consistency, reducing the burden of compliance with these requirements that apply to healthcare organizations.

HITRUST ensures the CSF stays relevant and current to the needs of organizations by regularly updating the CSF to incorporate new standards and regulations as authoritative sources. This draft Summary of Changes for the proposed 2014 CSF (v6) release includes changes based on feedback from the community and an updated set of cross-references and security requirements for the **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 4 (r4) Appendix J, Privacy Control Catalog: Privacy Controls, Enhancement, and Supplemental Guidance**.

> "With the increasing dependency on information systems, dramatic advances in information technologies, and significant growth in new applications of those technologies in such areas as cloud computing, smart grid, and mobile computing, information security and privacy are taking on new levels of importance in the public and private sectors…. In today's digital world, effective privacy for individuals depends on a solid foundation of information security safeguards in the information systems that are processing, storing, and transmitting personally identifiable information. Privacy and security controls … are complementary and mutually reinforcing in trying to achieve the privacy and security objectives of organizations." NIST SP 800-53 r4, App J

In the healthcare sector, it is expected that more reliance will continue to be placed on electronic health records (EHRs) and on interoperable health information exchanges (HIEs) to improve patient care, minimize errors, reduce disparities, control costs and support public health initiatives, among other goals. As more EHRs and HIEs take root, the healthcare industry must be able to protect patient privacy while supporting the flow of the health data in a way that benefits individuals and society.



In response to industry demand and with a view towards future needs, HITRUST is incorporating privacy requirements into the CSF to create an integrated security and privacy framework. This transformative enhancement to the CSF will ensure better alignment between healthcare organizations' security and privacy programs and ensure organizations have an integrated approach for protecting health information.

The changes in this Summary were developed by a health industry working group to establish a uniform and practical approach to implementing privacy controls, taking into account both risk and cost factors that organizations can adopt to ensure they adequately protect patient, family member, and workforce privacy.

After conducting a review of various privacy frameworks, the working group focused its efforts on the privacy controls contained in Appendix J of NIST SP 800-53 r4 as well as other privacy best practices recommended by organizations and experts that are relevant to the healthcare industry. Based on this assessment, the group recommended the inclusion of specific privacy control categories, objectives, specifications and requirements by implementation level and regulatory, organizational and system risk factors associated with those levels.

This Summary contains 125 changes affecting 35 controls in the CSF, with some of the most significant changes impacting confidentiality, consent and disclosure requirements in CSF control 06.d, Data Protection and Privacy of Covered Information.

Green text indicates an addition to the control/requirement. ~~Red~~ text indicates a deletion from the control/requirement.

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
00.a	Control Name	Updated: Information Protection ~~Security~~ Management Program	Administrative change	Incorporates privacy into the framework
00.a	1	Updated: An Information Protection ~~Security~~ Management Program (IPMP) ~~(ISMP)~~ shall be documented that addresses the overall security and privacy programs of the organization. Management support for the IPMP ~~ISMP~~ shall be demonstrated through signed acceptance or approval by management. The IPMP ~~ISMP~~ shall consider all the HITRUST Control Objectives and document any excluded control domains and the reasons for their exclusion. The IPMP ~~ISMP~~ shall be updated at least annually or when there are significant changes in the environment.	Administrative change	Incorporates privacy into the framework
00.a	2	Updated: The organization shall formally establish, implement, operate, monitor, review, maintain and improve the IPMP ~~ISMP~~. The IPMP ~~ISMP~~ shall be ... The IPMP ~~ISMP~~ shall incorporate a Plan, Do, Check, Act (PDCA) cycle for continuous improvement in the ISMP, particularly as information is obtained that could improve the IPMP ~~ISMP~~, or indicates any shortcomings of the IPMP ~~ISMP~~.	Administrative change	Incorporates privacy into the framework

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
00.a	3	Updated: Management shall provide evidence of its commitment to the … IPMP ~~ISMP~~. The organization shall determine and provide the resources needed to establish, implement, operate, monitor, review, maintain and improve an IPMP ~~ISMP~~. The organization shall ensure that all personnel who are assigned responsibilities defined in the IPMP ~~ISMP~~ are competent to perform the required tasks. The organization shall also ensure that all relevant personnel are aware … of their information security and privacy activities and how they contribute to the achievement of the IPMP ~~ISMP~~ objectives. The organization shall conduct internal IPMP ~~ISMP~~ audits at planned intervals ... Management shall review the organization's IPMP ~~ISMP~~ at planned intervals ... This review shall include assessing opportunities for improvement and the need for changes to the ISMP, including the information ~~security~~ protection policy and information security and privacy objectives. The results of the reviews shall be clearly documented and records maintained. The organization shall continually improve the effectiveness of the IPMP ~~ISMP~~ through the use of the information ~~security~~ protection policy, information security and privacy objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.	Administrative change	Incorporates privacy into the framework

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
01.c	1	Added: Users who have been previously terminated for cause from the organization are re-evaluated prior to privileges being re-enabled in a new job role within the organization or with another entity that has access to the organization's systems.	NIST SP 800-53 r4 AC-2	Added during Privacy Working Group Offsite; requirement is intended to address a specific threat stemming from personnel transfers (due to termination from a specific role for cause) within an organization or subsequent hiring by another covered entity or business associate with access to the organization's systems.
02.0	Control Category Name	Removed: Human Resources ~~Security~~	Administrative change	Modified for consistency with the integration of security and privacy
02.a	1	Updated: The organization shall develop, disseminate, and review/update annually: i. ~~a~~ formal, documented personnel security and privacy policy~~y~~ies that addresses purpose, … and compliance; and ii. formal, documented procedures to facilitate the implementation of the personnel ~~security policy~~ security and privacy policies and associated ~~personnel security~~ controls. Security roles and responsibilities shall include the following requirements: i. implement and act in accordance with the organization's information security and privacy policies; ii. protect assets from unauthorized access, disclosure, modification, destruction or interference; iii. execute particular security and privacy processes or activities; iv. ensure responsibility is assigned to the individual for actions taken; and	Administrative change	Added during Privacy Working Group Offsite

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		report security and privacy events or potential events or other security risks to the organization.		
02.a	1	Added: Security and privacy roles and responsibilities of employees, contractors and third party users shall be defined and ... NIST cross reference	NIST SP800-53 R4 AR-3 HIPAA Privacy Rule 45 CFR §164.530(b)(1)	Related to the existing requirement to establish security roles and responsibilities
02.a	2	Added: The pre-employment process shall be reviewed by recruitment to ensure security and privacy roles and responsibilities are defined and clearly communicated to job candidates. … The organization shall define the roles, responsibilities and authority of all security and privacy personnel.	NIST SP800-53 R4 AR-3 HIPAA Privacy Rule 45 CFR §164.530(b)(1)	Related to the existing requirement to establish security roles and responsibilities
~~02.b~~	~~1~~	~~Added:~~ ~~Verification checks shall … include the following:~~ • ~~Confirmation that candidate is eligible for user access rights.~~ • ~~…~~ ~~…~~ ~~Organizations shall define mechanisms to verify the candidate has not had their user access rights previously revoked by the organization or HIE and approves/denies access based upon documented policies and procedures.~~		~~Added during Privacy Working Group Offsite~~ HITRUST – Recommended change deleted as the requirements are outlined for the more general case in relevant controls, e.g., 02.b, 02.g, 02.h and 02.i.

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
02.d	1	Updated: Management responsibilities shall include ensuring that employees, contractors and third party users: i. are properly briefed on their information security and privacy roles and responsibilities prior to being granted access to covered information or information systems; ii. are provided with guidelines to state security and privacy expectations of their role within the organization; iii. are motivated and comply with the ~~security~~ information protection policies of the organization; iv. achieve a level of awareness on security and privacy relevant to their roles and responsibilities within the organization v. conform to the terms and conditions of employment, which includes the organization's information ~~security~~ protection policy and appropriate methods of working; and …		
02.d	1	Added: The organization shall use PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in the organization's public notices. NIST cross reference	NIST SP800-53 R4 UL-1 HIPAA Privacy Rule 45 CFR Part 164.502(b)	Related to the requirement for ensuring the workforce complies with relevant security policies and procedures
02.e	Control Name	Updated: Information Protection ~~Security~~ Awareness, Education, and Training	Administrative change	Facilitates incorporating privacy into the framework by making the term more generic

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
02.e	1	Updated: Awareness training shall commence with a formal induction process designed to introduce the organization's ~~security~~ information protection policies, state and federal laws, … Ongoing training shall include security and privacy requirements … NIST cross reference	NIST SP800-53 R4 AR-5 HIPAA Privacy Rule 45 CFR §164.530(b)(1)	Training requirements
02.e	2	Added: The organization formally creates dedicated ~~security~~ information protection awareness training ... The organization documents its formal induction ~~security~~ information protection awareness training process. The organization conducts an internal annual review of the effectiveness of its ~~security~~ information protection program. The organization manages an ~~security~~ information protection education and training program … The organization's security and privacy personnel, including organizational business unit security and privacy points of contact, shall receive specialized ~~security~~ information protection education and training appropriate to their role/responsibilities.	NIST SP800-53 R4 AR-5	Training requirements Not this specific in the Privacy Rule, but a best practice.
02.e	3	Added: The organization shall provide role-based ~~security~~ information protection-related training: i. … Personnel with significant information security and/or privacy roles and responsibilities shall be required to undergo appropriate information ~~system security~~ protection training: …	NIST SP800-53 R4 AR-5	Training requirements Not this specific in the Privacy Rule, but a best practice.

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
02.f	1	Updated: The organization employs a formal sanctions process … established information security and privacy policies and procedures. The disciplinary process … verification that a security or privacy policy violation ~~breach~~ has occurred. The formal disciplinary process shall ensure correct and fair treatment for employees who are suspected of committing ~~breaches~~ violations of security and privacy policies and procedures. The formal disciplinary process shall ... The organization shall maintain a list or document and indication of employees involved in security and privacy ~~incident~~ investigations and the resulting outcome in their HR folder.	Administrative change	Added during Privacy Working Group Offsite
03.a	1	Added: The organization shall develop, disseminate, and update reports to senior management and other personnel with responsibility for monitoring privacy program progress and compliance. NIST cross reference	NIST SP800-53 R4 AR-6	Management and reporting of privacy-related risk (e.g., regulatory non-compliance) is related to the management and reporting of security risk.

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
03.b	1	Added: The organization shall: i. document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII/PHI; and ii. conduct Privacy Impact Assessments (PIA) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy (if applicable), or any existing organizational policies and procedures. NIST cross reference	NIST SP800-53 R4 AR-2	Related to the requirement for security risk assessments
03.b	2	Added: CMS cross reference	CMSRs 2010v1.0 PL-5	Requirement moved from 03.b (Note PL-5 was withdrawn in NIST SP800-53 R4 and requirements incorporated into AR-2; this reference will be removed when CMS updates the ARS to reflect changes in R4)
04.0	Control Category Name	Updated: ~~Security~~ Protection Policy	Administrative change	Updated for consistency with the integration of security and privacy
04.a	Control Name	Updated: Information Protection ~~Security~~ Policy Document	Administrative change	Updated for consistency with the integration of security and privacy
04.a	1	Added: NIST cross reference	NIST SP800-53 R4 AR-1	Requirement to develop, disseminate and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies is addressed by 04.a

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
04.a	1	Updated: The information ~~security~~ protection policy document shall state management's commitment and establish the organization's approach to managing information security and privacy. The policy document shall contain statements concerning: i. a definition of information security and privacy, their ~~its~~ overall objectives and scope and the importance of security and privacy practices as an enabling mechanism for information sharing; ii. a statement of management intent, supporting the goals and principles of information security and privacy practices in line with the business strategy and objectives; iii. … iv. the need for information protection program for security and privacy; v. the goals of information ~~security~~ protection programs; … viii. arrangements for notification of information security and privacy incidents, including a channel for raising concerns regarding confidentially, without fear of blame or recrimination. ix. a brief explanation of the ~~security~~ information protection policies, principles, standards, and compliance requirements of particular importance to the organization, including: a. … b. security and privacy education, training … c. … d. consequences of information protection ~~security~~ policy violations; x. a definition … ~~security~~ information protection … xi. prescribes … of ~~security~~ information protection policy and associated security and privacy controls; and xii. references … detailed ~~security~~ information protection policies … or security and privacy rules …	Administrative change	Added during Privacy Working Group Offsite

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		The information ~~security~~ protection policy shall be communicated … to the intended reader.		
04.b	Control Name	Updated: Review of the Information Protection ~~Security~~ Policy	Administrative change	Updated for consistency with the integration of security and privacy
04.b	1	Added: NIST cross reference	NIST SP800-53 R4 AR-1	Requirements for a strategic plan and to periodically update privacy plan, policies, and procedures at an organization-defined frequency are addressed by 04.b
04.b	1	Updated: An information ~~security~~ protection policy shall be developed … for all aspects of security and privacy. The information ~~security~~ protection policy shall be reviewed at planned intervals … and effectiveness. Additional factors when developing or changing an information ~~security~~ protection policy shall include, but are not limited to … A process shall be defined … concerning the information ~~security~~ protection policies and procedures or the organization's compliance with the policies …	Administrative change	Updated for consistency with the integration of security and privacy
04.b	2	Updated: An information ~~security~~ protection policy shall be reviewed at planned intervals, at a minimum annually… The information ~~security~~ protection policy shall have an owner … and evaluation of the ~~security~~ policy. The review shall include … the organization's information ~~security~~ protection policy and approach to managing information ~~security~~ protection in response to changes … or technical	Administrative change	Updated for consistency with the integration of security and privacy

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		environment. There shall be defined management review procedures of the information ~~security~~ protection policy including a schedule ... The input to the management review shall include information on: … v. process performance and information ~~security~~ protection policy compliance; vi. changes that could affect the organization's approach to managing information security and privacy … … viii. reported information security and privacy incidents (see 11.a); and ix. … The output from the management review shall include any decisions and actions related to: i. improvement of the organization's approach to managing information ~~security~~ protection and its processes; ii. …		
05.0	Control Category Name	Added: Organization of Information Security and Privacy	Administrative change	Updated for consistency with the integration of security and privacy
05.a	Control Name	Updated: Management Commitment to Information Protection ~~Security~~	Administrative change	Updated for consistency with the integration of security and privacy
05.a	1	Added: The organization's senior management shall:	NIST SP800-53 R4 AR-1	Added during Privacy Working Group Offsite: identifies the need for a senior-level privacy official (who may or may not be dual-hatted as the security official) and expands

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		i. appoint (a) senior-level information security and privacy official(s); ii. ensure that the organization's information security processes are in place, are communicated to all stakeholders, and consider and address organizational requirements; ensure the senior privacy official develops, implements and maintains an organization-wide governance and privacy program compliant with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII/PHI by programs and information systems; iii. formally assign an organization single point of contact … information security and privacy risk … etc.); iv. formulate, review, and approve information ~~security~~ protection policy and a policy exception process; v. periodically, at a minimum, annually, review and assess the effectiveness of the implementation of the information ~~security~~ protection policy; vi. provide clear direction and visible management support for security and privacy initiatives; vii. provide the resources needed for information security and privacy; viii. initiate plans and programs to maintain information ~~security~~ protection awareness; ix. … ; x. ensure that the implementation of information security and privacy controls is coordinated across the organization; and xi. determine and coordinate, as needed, internal or external information security and privacy specialists, and review and coordinate results of the specialists' advice throughout the organization. The organization shall: i. ensure that all capital planning and investment requests include the resources needed to implement		on the privacy official's requirements HITRUST comment: language around the security processes, communication, and organizational requirements is provided in 04.a and processes are evaluated per the maturity model

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		the information ~~security~~ protection program and documents all exceptions to this requirement; ii. … ; and iii. ensure that information security and privacy resources are available for expenditure as planned. NIST cross reference		
05.a	2	Updated: i. ensure that organization's information ~~security~~ protection strategy … and goals; ii. formally review … any information ~~security~~ protection and risk management programs; iii. formally approve … information ~~security~~ protection across the organization; iv. formally appoint an employee … administration of security and privacy matters. The appointed lead shall … a recognized security and/or privacy industry certification, … ; and v. conduct an annual review (may be performed by a third party) of the effectiveness of its ~~security~~ information protection program. The information protection ~~security~~ planning policy shall be reviewed/updated annually. The organization shall formally appoint in … security and/or privacy contacts by name (may be dual-hatted) in each major organizational area or business unit.	Administrative change	Updated for consistency with the integration of security and privacy
05.a	3	Updated: i. the organization formally creates a dedicated security and privacy management forum and publishes the forum's member list and charter. Such responsibilities	Administrative change	Updated for consistency with the integration of security and privacy

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		can be handled by a Security and Privacy Advisory Board, Security and Privacy Steering Committee or by an existing management body, such as the board of directors; ii. the organization conducts an annual assessment of the effectiveness of its ~~security~~ information protection program performed by a qualified outside organization; iii. the organization shall publish security and privacy guidelines and/or daily operational procedures relating to processes that complement, clarify and enforce ~~security~~ information protection policies.		
05.b	Control Name	Updated: Information Protection ~~Security~~ Coordination	Administrative change	Updated for consistency with the integration of security and privacy
05.b	1	Added: NIST cross reference	NIST SP800-53 R4 AR-1	Requirement for organizationally-defined budget and staffing resources to implement and operate the organization-wide protection program is addressed by 05.b
05.b	1	Updated: The organization shall: i. determine information security and privacy … ii. … and iii. establish a discrete line item for information security and privacy in organizational programming and budgeting documentation. Information security and privacy coordination shall … This activity shall: i. ensure that security and privacy activities across the entire organization are executed in compliance with the	Administrative change	Added during Privacy Working Group Offsite

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		information ~~security~~ protection policy and that deviations are identified and reviewed; ii. … ; iii. assess the adequacy and coordinate the implementation of information security and privacy controls; iv. effectively promote information security and privacy education, training and awareness throughout the organization. Security and privacy-related activities affecting the information system environment shall be planned and coordinated …		
05.b	1	Added: The organization shall implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices. NIST cross reference	NIST SP800-53 R4 IP-4 HIPAA Privacy Rule 164.530 d(1) HIPAA Privacy Rule 164.520	Related to the requirement for internal incident reporting and security policy clarification
05.b	2	Updated: Information security and privacy coordination shall involve ... Information security and privacy coordination shall also include specialist skills in areas such as insurance, legal issues, human resources, ~~privacy,~~ IT or risk management. This activity shall: i. … ; ii. approve methodologies and processes for information security and privacy management activities (e.g. risk acceptance, information classification, security and privacy incidents);	Administrative change	Updated for consistency with the integration of security and privacy

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		iii. … ; iv. evaluate information received from the monitoring and reviewing of information security and privacy incidents to conduct "lessons learned" activities, and recommend to senior management appropriate actions in response to identified ~~information security~~ incidents. v. identify by name or position non-professional or professional security and privacy contacts in each major organizational area or business unit (may be dual-hatted); vi. create an internal security and privacy information sharing mechanism, such as an e-mail group, periodic conference call or standing meeting; vii. establish an internal reporting mechanism, such as a telephone hotline or dedicated e-mail address, to allow security and privacy contacts to report information security and privacy incidents or obtain ~~security~~ information protection policy clarifications on a timely basis. The organization develops an ~~security~~ information protection plan for the information system that: … iv. provides the security and privacy categorization of the information system including supporting rationale; … vii. provides an overview of the security and privacy requirements for the system; viii. describes the security and privacy controls in place or planned for meeting those requirements including a rationale for tailoring and supplementation decisions; ix. … The organization shall update the system security plan:		

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		… iv. after the occurrence of a serious security and/or privacy violation which raises questions about the validity of an earlier security and privacy authorization; and v. prior to expiration of a previous security and privacy authorization. The organization shall plan and coordinate security and privacy-related activities affecting the information system … The organization shall: i. distribute copies of the information system's ~~security~~ information protection plan to appropriate individuals and offices (e.g., CCO, CIO, business units) and ii. communicate any changes to the communicate any changes to the ~~security~~ information protection plans (see 05.b) to appropriate individuals and offices.		
05.b	2	Added: The organization shall respond to complaints, concerns, or questions from individuals within a formally specified time period. NIST cross reference	NIST SP800-53 R4 IP-4(1)	Enhancement to the process requirement
05.b	3	Updated: The organization shall convene an internal meeting for the organization's security single point(s) of contact for security and privacy and the organizational area/business unit security and privacy contacts (see 05.a) on a monthly or near to monthly basis.	Administrative change	Updated for consistency with the integration of security and privacy
05.d	1	Updated: The following shall be required for the authorization process:	Administrative change	Updates required to support language changes in 05.b regarding system authorization

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		i. new information processing assets … and use. Authorization shall also be obtained from the manager responsible for maintaining the local information system security and privacy environment to ensure that all relevant ~~security~~ information protection policies and requirements are met; ii. information assets shall have appropriate security and privacy measures commensurate with … iii. …		
05.d	2	Updated: The following shall be required for the authorization process: i. the organization shall establish a security and privacy authorization process and checklist for all new assets and facilities; ii. the organization shall establish policies and procedures to include the security and privacy organization(s) in procurement considerations for new IT equipment; iii. …	Administrative change	Updates required to support language changes in 05.b regarding system authorization
05.d	3	Updated: All new facilities shall undergo a site security and privacy survey by the organization's security and privacy department(s) or a trusted third party, and resolve all security and privacy shortcomings before any covered information is processed at that location …	Administrative change	Updates required to support language changes in 05.b regarding system authorization
05.f	1	Added: The organization should define a plan with associated contact information for reporting security or privacy incidents to law enforcement if it is expected that laws may have been broken.	Administrative change	Updated based on Privacy Working Group Offsite and subsequent comments by Working Group members

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
05.f	2	Added: Each group … and how identified information security and privacy incidents shall be reported in a timely manner if it is suspected that laws may have been broken.	Administrative change	Updated based on Privacy Working Group Offsite and subsequent comments by Working Group members
05.g	1	Added: Membership in organization-defined special interest groups or forums shall be considered as a means to: i. improve knowledge about best practices and staying up to date with relevant security and privacy information; ii. ensure the understanding of the information security and privacy environments is current and complete; iii. receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities; iv. gain access to specialist information security and privacy advice;	Administrative change	Added during Privacy Working Group Offsite
05.i	1	Added: The organization shall: i. share personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or in a manner compatible with those purposes; ii. where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; iii. monitor, audit and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and	NIST SP800-53 R4 UL-2 HIPAA Privacy Rule 45 CFR Part 164.504 (e)(1)	Related to the requirements for due diligence around information sharing

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		iv. evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required. NIST cross reference		
05.i	1	Added: Due diligence shall be carried out to identify any requirements for specific security and privacy controls where access by external parties is required. The identification of security and privacy risks related to external party access shall take into account the following issues: … Access by external parties … and conditions for the connection or access and the working arrangement. All security and privacy requirements resulting from … shall be secured via encrypted channels (e.g. VPN)… External parties shall be granted minimum necessary access to the organization's information assets to minimize risks to security and privacy. All access … revoked when no longer needed. It shall be ensured that the external party is aware of their obligations, and accepts the security and privacy responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets. NIST cross reference	NIST SP800-53 R4 AR-3 HIPAA Privacy Rule 45 CFR §164.314 and 164.510	Related to existing security third party requirements

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
05.i	2	Added: The organization shall monitor the information system connections on an ongoing basis, verifying enforcement of security and privacy requirements.	NIST SP800-53 R4 AR-3 HIPAA Privacy Rule 45 CFR §164.314 and 164.510	Related to existing security third party requirements
05.j	Control Name	Updated: Addressing Security and Privacy When Dealing with Customers	Administrative change	Updated for consistency and to reflect the inclusion of privacy requirements around notice and consent
05.j	1	Updated: The following ~~security~~ terms shall be addressed prior to giving customers access to any of the organization's assets: … The organization shall permit an individual to request to restrict the disclosure of the individual's covered data ~~to a business associate~~ for purposes of carrying out payment or health care operations, ~~and is~~ but not for purposes of carrying out treatment. The organization shall respond to ~~any~~ requests from an individual ~~on the disclosure of the individual's covered data~~, ~~to~~ providing provide ~~the individual with~~ records (see 06.c) of disclosures of covered data that are made by the organization and either: i. records (see 06.c) of disclosures of covered data made by a business associate acting on behalf of the organization; or ii. a list of ~~all~~ business associates acting on behalf of the covered entity for that individual, including contact	Administrative change	Edited due to Privacy Working Group Offsite meeting – From a HIPAA perspective, it's not always to a business associate – for example, a request for restriction to not include services to a health plan for which the individual has paid in full – the health plan is not a business associate – it's a covered entity

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		information for such business associates (such as mailing address, phone, and email address).		
05.j	1	Added: The organization shall: i. provide individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records; ii. publish rules and regulations governing how individuals may request access to by the organization; and iii. publish access procedures in System of Records Notices (SORNs) or Notice of Privacy Practices. NIST cross reference	NIST SP800-53 R4 IP-2 HIPAA Privacy Rule 45 CFR Part 164.524	Related to the controls required prior to giving access to customers to protect organizational assets.
05.j	1	Added: The organization shall: i. provide a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and ii. establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifying affected individuals that their information has been corrected or amended. NIST cross reference	NIST SP800-53 R4 IP-3 HIPAA Privacy Rule 45 CFR Part 164.526	Related to the requirement for making “arrangements for reporting, notification, and investigation of information inaccuracies …”

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
05.j	1	Added: The organization shall develop, publish and maintain a public System of Records Notice (SORN) or Notice of Privacy Practices. Government agencies and contractors subject to the Privacy Act shall i. ensure their SORNs are consistent with the Act, and ii. include Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected NIST cross reference	NIST SP800-53 R4 TR-2	Notice and consent requirements addressed in 05.j; confidentiality and disclosure is addressed in 06.d Privacy Working Group wanted to delete the Privacy Act requirements as they generally do not apply to commercial entities HITRUST recommends qualifying the requirement rather than removing it in its entirety
05.j	1	Added: The organization shall ensure that: i. the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and ii. Its privacy practices are publicly available through organizational Web sites or otherwise. NIST cross reference	NIST SP800-53 R4 TR-3 HIPAA Privacy Rule 45 CFR Part 160.520 HIPAA Privacy Rule 45 CFR Part 164.530(a)(i) HIPAA Privacy Rule 45 CFR Part 164.530(a)(ii)	Notice and consent requirements addressed in 05.j; confidentiality and disclosure is addressed in 06.d

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
05.j	1	Added: Where required by legislation, consent shall be obtained … to the organization. The organization shall: i. provide a means, where feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of personally identifiable information (PII) prior to its collection; ii. provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; iii. obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and iv. ensure that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII. NIST cross reference	NIST SP800-53 R4 IP-1 HIPAA Privacy Rule 45 CFR Part 164.508(a) HIPAA Privacy Rule 45 CFR Part 164.506	Related to the requirement for consent
05.j	2	Added: The organization shall limit the collection of PII/PHI to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent.(see 06.d),	NIST SP800-53 R4 DM-1 HIPAA Privacy Rule 45 CFR Part 164.502(b)	Related to the requirement for minimal use of PII/PHI

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
05.j	1	Added: The organization shall: i. confirm to the greatest extent practicable upon collection or creation of PII/PHI, the accuracy, relevance, timeliness, and completeness of that information; and ii. collect PII/PHI directly from the individual to the greatest extent practicable; NIST cross reference	NIST SP800-53 R4 DI-1	Specific to data quality during the collection process
05.j	1	Added: The organization shall request that the individual or individual's authorized representative validate PII during the collection process. NIST cross reference	NIST SP800-53 R4 DI-1(1)	Enhances requirements for ensuring data quality during the collection process.
05.j	2	Added: Government agencies and contractors subject to the Privacy Act shall publish SORNs on its Public Web site. NIST cross reference	NIST SP800-53 R4 TR-2(1)	Enhancement to the SORN requirement for government agencies and others subject to the Privacy Act
05.j	2	Added: The organization shall implement mechanisms to support itemized or tiered consent for specific uses of data. NIST cross reference	NIST SP800-53 R4 IP-1(1) HIPAA Privacy Rule 45 CFR Part 164.508(b)(iii) HIPAA Privacy Rule 45 CFR Part 164.512	Related to the requirement for consent

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
05.j	2	Added: The organization shall periodically request that the individual or individual's authorized representative revalidate that PII collected is still accurate at a frequency specified by the organization but no less than annually. NIST cross reference	NIST SP800-53 R4 DI-1(2)	Enhances the requirement to ensure data quality
05.j	1	Added: The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices. NIST cross reference	NIST SP800-53 R4 AP-2 HIPAA Privacy Rule 45 CFR Part 160.520	Related to the inclusion of privacy requirements in notices required by TR-1; notice, consent and collection is being addressed in 05.j
05.j	1	Added: The organization shall: i. provide effective notice to the public and to individuals regarding: (1) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (2) authority for collecting PII; (3) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (4) the ability to access and have PII amended or corrected if necessary; ii. describe: (1) the PII the organization collects and the purpose(s) for which it collects that information; (2) how the organization uses PII internally; (3) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (4) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (5) how individuals may obtain access to PII; and (6) how the PII will be protected; and	NIST SP800-53 R4 TR-1 HIPAA Privacy Rule 45 CFR Part 160.520	Notice, consent and collection is being addressed in 05.j

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		iii. revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change. NIST cross reference		
05.j	2	Added: The organization shall provide real-time and/or layered notice when it collects PII. NIST cross reference	NIST SP800-53 R4 TR-1(1) HIPAA Privacy Rule 45 CFR Part 160.520	Related to the requirement to use computer login banners that users must acknowledge; notice, consent and collection is being addressed in 05.j
05.k	Control Name	Added: Addressing Security and Privacy in Third Party Agreements	Administrative change	Updated for consistency with the integration of security and privacy
05.k	1	Updated: The following terms shall be implemented for inclusion in the agreement in order to satisfy the identified security and privacy requirements (see 5.i): i. the information security and privacy policy~~y~~ies; … ix. access control policy, covering: 1. ~~the different reasons, requirements, and benefits~~ the business justification for 3rd party access to restricted systems in accordance with the principal of least privilege ~~that make the access by the third party necessary;~~ … x. arrangements for reporting, notification, and investigation of information security and privacy incidents and ~~security~~ breaches, as well as violations of the requirements stated in the agreement, …	Administrative change	Added during Privacy Working Group Offsite; made language more restrictive consistent with best practice

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
06.a	1	All relevant statutory, regulatory and contractual requirements shall be explicitly defined and documented ~~within formal policies and procedures~~ for each information system type. The specific controls and individual responsibilities to meet these requirements shall be similarly defined and documented. These controls shall be communicated to the user community through the documented security training and awareness programs.	CSA CCM v1.0 CO-5	Privacy Working Group comments: This control may be considered a roadblock to adoption of the CSF due to the highlighted portions HITRUST comment: CO-5 does not indicate where the requirements for each information type (element) must be specified; however, the rneed to specify the requirements will be documented in policy and supported by procedures IAW the HITRUST maturity model.
06.a	1	Added: NIST cross reference	NIST SP800-53 R4 AR-1	Requirement to monitor federal and state privacy laws and policy for changes that affect the privacy program is addressed by 06.a and 04.b
06.a	1	Added: The organization shall determine the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need. NIST cross reference	NIST SP800-53 R4 AP-1 HIPAA Privacy Rule 45 CFR Part 164 *(referring to entire Privacy Rule)*	Related to the requirement for legislative requirements to be clearly defined, documented and communicated to the user

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
06.c	1	Added: The organization shall: i. retain each collection of PII/PHI for a time-period defined by the organization to fulfill the purpose(s) identified in their privacy notice or as required by law; ii. dispose of, destroy, erase, and/or anonymize the PII/PHI, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and iii. use techniques or methods specified and approved by the organization to ensure secure deletion or destruction of PII (including originals, copies, and archived records). NIST cross reference	NIST SP800-53 R4 DM-2 HIPAA Privacy Rule 45 CFR Part 164.530 (c) & (j)	Related to the existing requirements addressing retention in Level 1 and disposal policies and procedures in Level 2
06.c	2	Added: The organization shall, where feasible, configure its information systems to record the date PII/PHI is collected, created, or updated and when PII/PHI is to be deleted or archived under an approved record retention schedule. NIST cross reference	NIST SP800-53 R4 DM-2(1)	Enhancement to the retention requirements in DM-2
06.d	Control Name	Updated: Data Protection and Privacy of ~~Covered~~ Personal Information	Administrative change	Updated to reflect the inclusion of PII
06.d	1	Removed: An organizational data protection and privacy policy shall be developed and implemented. This policy shall be communicated to all persons involved in the processing of covered information. Compliance with this policy and all relevant data protection legislation and regulations shall be supported by management structure and control. Responsibility for handling covered information and ensuring	CSA IS-18 Guidance to render PHI unusable, unreadable, or indecipherable (a)(i) Guidance to render PHI unusable, unreadable, or indecipherable (a)(ii) ISO/IEC 27002-2005 15.1.4 ISO 27799-2008 7.12.2.2	Per Privacy Working Group Offsite: Remove current language in 06.d to accommodate the many additions being proposed in this document. HITRUST comments: Policy and the communication of policy are addressed in 04.a; leadership structure/control is addressed in

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		awareness of the data protection principles shall be dealt with in accordance with relevant legislation and regulations. Technical security controls, including access controls and monitoring, and organizational measures to protect covered information shall be implemented. There shall be an appointment of a person responsible, such as a data protection officer, who shall provide guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that shall be followed. Where required by legislation, consent shall be obtained before any protected information (e.g. about a patient) is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the organization.	JCAHO IM.02.01.03, EP 2 NRS 603A.210.1	04.a and 05.a; relevant legislation and regulations is addressed in 06.a and 06.c; awareness is addressed in 02.e; technical security controls supporting the protection of covered information are addressed in multiple controls; appointment of a data protection officer is addressed in 05.a; consent is addressed in 05.j. CSF Control 06.d will be used to document confidentiality and privacy requirements for the processing and sharing of PII and PHI
06.d	1	Added: Organizations shall formally specify 'Rights' for individuals who are the subject of PII/PHI, including but not limited to the following: notification of the entities privacy practices; accessing, amending and restricting access to their PII/PHI; use and disclosure policies; means for authorizing release and revocation of release; means for requesting how an entity will communicate with the individual; obtaining an accounting of disclosures of their information; and a means for opting out of communications. Organizations releasing PII/PHI shall ensure only valid authorizations are honored, excluding disclosures for treatment, payment and health care operations and to appropriate vendors with a valid business associate agreement arrangement and organized health care arrangements (OHCAs).	HIPAA Privacy Rule 45 CFR Part 164 (referring to entire Privacy Rule)	Per Privacy Working Group Offsite: Added to accommodate basic HIPAA Rights, authorizations and disclosures not mentioned in the NIST appendix.

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		Disclosures of such PII/PHI will be the minimum necessary amount needed for each specific task, with the exception of the individual who is subject of the information or to their personal representative. Authentication procedures must reasonably and appropriately identify individuals prior to disclosure of any information.		
06.d	CMS	Removed: The organization shall conduct a Privacy Impact Assessment (PIA) on the information system in accordance with OMB policy. CMS cross reference	CMSRs 2010v1.0 PL-5	Requirement moved to 03.b
06.d	1	Added: The organization shall: i. minimize the use of personally identifiable information (PII) for testing, training, and research; and ii. implement controls to protect PII used for testing, training, and research. NIST cross reference	NIST SP800-53 R4 DM-3 HIPAA Privacy Rule 45 CFR Part 164.502(b) HIPAA Privacy Rule 45 CFR Part 164.530(i)(1)	Related to the requirement in DM-1 for minimal use of covered information
06.d	1	Added: The organization shall: i. periodically check for, and correct as necessary, any inaccurate or outdated PII used by its programs or systems at a frequency specified by the organization, but no less than annually; and ii. issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. NIST cross reference	NIST SP800-53 R4 DI-1	Related to organizational-level privacy requirements for covered information; although integrity is a component of data quality, data integrity requirements are addressed in DI-2, which is mapped to 06.d and 10.b, c and d

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
06.d	1	Added: The organization shall: i. keep an accurate accounting of disclosures of information held in each system of records under its control, including: 1. date, nature, and purpose of each disclosure of a record, and 2. name and address of the person or agency to which the disclosure was made; ii. retain the accounting of disclosures for six years, and iii. make the accounting of disclosures available to the person named in the record upon request. NIST cross reference	NIST SP800-53 R4 AR-8 HIPAA Privacy Rule 45 CFR §164.528	Requirements for confidentiality and disclosure of PII/PHI is addressed in 06.d; Privacy Working Group Offsite modified the NIST requirement from 5 to 6 years per HIPAA Privacy Rule
06.d	1	Added: The organization shall document processes to ensure the integrity of personally identifiable information (PII) through existing security controls (e.g., 10.c). NIST cross reference	NIST SP800-53 R4 DI-2	Related to the organizational-level privacy requirements for data integrity; specific data integrity requirements are outlined in 10.b, 10.c and 10.e
06.d	2	Added: The organization shall: i. identify the minimum PII/PHI elements that are relevant and necessary to accomplish the legally authorized purpose of collection; ii. conduct an initial evaluation of PII/PHI holdings; and iii. establish and follow a schedule for regularly reviewing those holdings, at least annually, to ensure that only PII/PHI identified in the notice is collected (per 05.j) and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose. NIST cross reference	NIST SP800-53 R4 DM-1 HIPAA Privacy Rule 45 CFR Part 164.502(b)	Related to the requirement for minimal use of PII/PHI Privacy Working group recommended deleting the Privacy Act-related requirements HITRUST recommends making the requirements generic and provide a best practice rather than removing them entirely

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
06.d	2	Added: The organization, where feasible and within the limits of technology, shall locate and remove/redact specified PII and/or use anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and the risk resulting from unauthorized disclosure. NIST cross reference	NIST SP800-53 R4 DM-1(1) HIPAA Privacy Rule 45 CFR Part 164.502(d) HIPAA Privacy Rule 45 CFR Part 164.514 (a) & (b)	Enhancement is related to the requirement for minimizing the storage of covered information
06.d	2	Added: The organization shall, where feasible, uses techniques such as de-identification to minimize the risk to privacy of using PII for research, testing, or training. NIST cross reference	NIST SP800-53 R4 DM-3(1) HIPAA Privacy Rule 45 CFR Part 164.502(d)	Enhancement to the requirement for minimal use of covered information
06.d	2	Added: For government organizations and contractors subject to the Privacy Act, the organization shall establish a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements (e.g., a computerized comparison of two or more automated systems of records) and to ensure that those agreements comply with the computer matching provisions of the Act.	NIST SP800-53 R4 DI-2	Related to the organizational-level privacy requirements for data integrity; specific data integrity requirements are outlined in 10.b, 10.c and 10.e
06.g	Control Name	Added: Compliance with Security and Privacy Policies and Standards	Administrative change	Updated for consistency with the integration of security and privacy

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
06.g	1	Added: Reviews of the compliance of systems with security and privacy policies, standards and any other security and privacy requirements (HIPAA, legal, etc.)... Compliance reviews shall be conducted by security/privacy or audit individuals and will incorporate reviews of documented evidence. Annual security and privacy compliance assessments shall be conducted to ensure effective implementation of related controls. NIST cross reference	NIST SP800-53 R4 AR-4 HIPAA Privacy Rule 45 CFR §164.314 and 164.510	Privacy monitoring and auditing is related to the requirement for compliance reviews and assessments
06.g	2	Added: The internal security and privacy organization(s) shall regularly review the compliance … The organization shall employ assessors or assessment teams to monitor the security and privacy controls in the information system on an ongoing basis … Results of reviews and corrective actions carried out shall be recorded and these records shall be maintained. The security and privacy organization(s) shall maintain records of the compliance results in order to better track security and privacy trends within the organization and to address longer term areas of concern. The security and privacy organization(s) shall maintain records of the compliance results (e.g., organization-defined metrics) in order to better track security and privacy trends within the organization, respond to the results of correlation and analysis, and to address longer term areas of concern.	NIST SP800-53 R4 AR-4 HIPAA Privacy Rule 45 CFR §164.314 and 164.510	Privacy monitoring and auditing is related to the requirement for compliance reviews and assessments

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
07.a	1	Added: The organization shall periodically, at an organizationally-defined frequency, but no than less annually: i. identify all assets including information and document the importance of these assets; ii. establish, maintain, and update an inventory that: i. contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII/PHI; and ii. include all information necessary in order to recover from a disaster, including type or classification of the asset, format, location, backup information, license information, and a business value: and iii. provide each update of the asset inventory to the CIO or information security official to support the establishment of information security requirements for all new or modified information systems containing PII/PHI or other sensitive information (see 07.d). ~~The asset inventories shall include … and a business value.~~ The inventory shall not duplicate other inventories unnecessarily, but it shall be ensured that the content is aligned. NIST cross reference	NIST SP800-53 R4 SE-1	Related to requirements for an asset inventory
09.e	1	Added: iii. security and privacy controls, including third-party personnel security, information classification, transmission, and authorization; and NIST cross reference	NIST SP800-53 R4 AR-3 HIPAA Privacy Rule 45 CFR §164.314 and 164.510	Service delivery related to third party contracts

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
09.e	2	Added: In the case of outsourcing arrangements, the organization shall … ensure that security and privacy is maintained throughout the transition period…	NIST SP800-53 R4 AR-3 HIPAA Privacy Rule 45 CFR §164.314 and 164.510	Service delivery related to third party contracts
09.t	1	Added: vii. Responsibilities and liabilities in the event of information security and privacy incidents, such as loss of data; NIST cross reference	NIST SP800-53 R4 AR-3 HIPAA Privacy Rule 45 CFR § 164.314 and 164.510	Related to existing requirements for roles and responsibilities for security incidents
09.aa	1	Updated: Information systems processing PII/PHI ~~covered information~~ shall create a secure audit record each time a user accesses, creates, updates, or archives PII/PHI ~~covered information~~ via the system. Audit logs shall not include more than the minimum necessary PII/PHI to support business operations.	NIST SP800-53 R4 AR-4	Audit log requirement added during Privacy Work Group offsite.
10.01	Control Objective Name	Added: Security and Privacy Requirements of Information Systems	Administrative change	Updated for consistency with the integration of security and privacy
10.a	Control Name	Added: Security and Privacy Requirements Analysis and Specification	Administrative change	Updated for consistency with the integration of security and privacy
10.a	1	Added: Contracts and other acquisition-related documents with the supplier shall include the identified security and privacy requirements. NIST cross reference	NIST SP800-53 R4 AR-3 HIPAA Privacy Rule 45 CFR §164.314 and 164.510	Related to existing security requirements for exchange agreements

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
10.a	1	Added: Specifications for ~~the~~ security and privacy control requirements shall include that security and privacy controls be incorporated in the information system, ... Security and privacy requirements and controls shall reflect the business value of the information assets involved (see 7.d), and the potential business damage that might result from a failure or absence of security and privacy. For purchased commercial product, a formal acquisition process shall be followed. Contracts with the supplier shall include the identified security and privacy requirements. Where the security and privacy functionality in a proposed product ... Where additional functionality is supplied and causes a security or privacy risk, this shall be disabled or mitigated through application of additional controls. Controls shall be automated where possible. NIST cross reference	NIST SP800-53 R4 AR-7	Related to the specification of security controls
10.a	2	Added: The organization shall apply information system security engineering principles … security and privacy requirements and controls in developed and acquired information systems. Specifications for the security and privacy control requirements shall include … System requirements for information security and privacy and processes for implementing security and privacy shall be integrated in the requirements definition phase… Commercial products sought to store and/or process covered information shall undergo a security and privacy assessment and/or security and privacy certification by a qualified assessor prior to implementation. (Not applicable to operating system software).	NIST SP800-53 R4 AR-7	Related to the specification of security controls

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		Information security and privacy roles and responsibilities are defined … The organization's ~~security~~ risk management process shall be integrated into all SDLC activities. System requirements for information security and privacy and processes for implementing security and privacy shall be integrated in the requirements definition phase.		
10.a	3	Added: The organization develops enterprise architecture with consideration for information security and privacy … … The organization shall include security and privacy functional, strength and assurance requirements and security and privacy-related documentation requirements …	NIST SP800-53 R4 AR-7	Related to the specification of security controls
10.b	1	Added: NIST cross reference	NIST SP800-53 R4 DI-2	Related to existing data integrity requirements for input data validation
10.c	1	Added: NIST cross reference	NIST SP800-53 R4 DI-2	Related to existing data integrity requirements for internal processing
10.e	1	Added: NIST cross reference	NIST SP800-53 R4 DI-2	Related to existing data integrity requirements for data output validation
11.0	Control Category Name	Added: Information Security and Privacy Incident Management	Administrative change	Updated for consistency with the integration of security and privacy
11.01	Control Objective Name	Added: Reporting Information Security and Privacy Incidents and Weaknesses	Administrative change	Updated for consistency with the integration of security and privacy
11.a	Control Name	Added: Reporting Information Security and Privacy Events	Administrative change	Updated for consistency with the integration of security and privacy

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
11.a	1	Added: Formal information security and privacy event reporting procedures to support the corporate direction (policy) shall be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security or privacy event, . . . A point of contact shall be established for the reporting of information security and privacy events. It shall be ensured that this (these) point(s) of contact is (are) known throughout the organization, is (are) always available and ~~is~~ able to provide adequate and timely response. Employees and other workforce members, including third parties, are able to freely report information security and privacy events or concerns (real and perceived) without fear or repercussion. The organization shall implement an insider threat program that includes a cross-discipline insider threat incident handling team for information security and privacy events.	Administrative change	Added during Privacy Working Group Offsite
11.a	2	Added: … The organization shall institute a mechanism to anonymously report security and privacy issues. Procedures shall be developed to provide for definition of the information security and privacy incidents … and communication processes. They shall also state the requirements for … the handling of third party security and privacy breaches… All employees … are aware of their responsibilities to report any information security and privacy events as quickly as possible, the procedure for reporting information security and privacy events and the point(s) of contact. The reporting procedures shall include:	Administrative change	Updated for consistency with the integration of security and privacy

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
		i. feedback processes to ensure that those reporting information security and privacy events … ; ii. information security and privacy event reporting … in case of an information security and/or privacy event including: 1. the correct behavior to be undertaken in case of an information security and/or privacy event … ; and 2. … ; iii. reference to … security and/or privacy breaches; iv. … … Alerts from the organization's intrusion-detection and intrusion-prevention systems shall be utilized for reporting information security and/or privacy events.		
11.a	3	Added: An information security and privacy assessment shall be made either on all incidents or …	Administrative change	Updated for consistency with the integration of security and privacy
11.c	1	Added: The organization shall develop ~~and document incident response policies and procedures.~~ a formal capability for an organized and effective response to security and privacy incidents. Organizations shall be capable of responsding to different types of information security and privacy incidents including: … NIST cross reference	NIST SP800-53 R4 SE-2	Related to requirements for security incident response

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
11.c	2	Added: Action to recover from security and privacy breaches and correct system failures shall be carefully and formally controlled… … In addition to reporting of information security and privacy events and weaknesses … NIST cross reference	NIST SP800-53 R4 SE-2	Related to requirements for security incident response
11.02	Control Objective Name	Added: Management of Information Security and Privacy Incidents and Improvements	Administrative change	Updated for consistency with the integration of security and privacy
11.d	Control Name	Added: Learning from Information Security and Privacy Incidents	Administrative change	Updated for consistency with the integration of security and privacy
11.d	1	Added: The information gained from the evaluation of information security and privacy incidents shall be used to identify recurring or high impact incidents. NIST cross reference	NIST SP800-53 R4 SE-2	Related to requirements for security incident response
11.d	2	Added: The organization shall: ~~1~~i. implement an incident handling capability for security and privacy incidents that includes detection and analysis, containment, eradication, and recovery; ~~2~~ii. … ~~3~~iii. … NIST cross reference	NIST SP800-53 R4 SE-2	Related to requirements for security incident response

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
12.01	Control Objective Name	Updated: Information ~~Security~~ Protection Aspects of Business Continuity Management	Administrative change	Updated for consistency with the integration of security and privacy
12.a	Control Name	Added: Including Information Security and Privacy in the Business Continuity Management Process	Administrative change	Updated for consistency with the integration of security and privacy
12.a	1	Added: … iv. formulating and documenting business continuity plans addressing information security and privacy requirements in line with the agreed business continuity strategy (see 12.c);	Administrative change	Added during Privacy Working Group Offsite
12.a	12	Added: … iii. understanding the impact which interruptions caused by information security and privacy incidents are likely to have on the business … ;	Administrative change	Added during Privacy Working Group Offsite
12.b	1	Updated: The Business Continuity Risk Assessment process ~~This process~~ shall identify ~~the~~ critical business processes and regulatory compliance obligations of the organization. Information security aspects of business continuity … of terrorism). This shall be followed by a risk assessment … time, damage scale and recovery period. The risk assessment shall also consider privacy requirements, such as the probability and impact of an unauthorized disclosure of PII/PHI due to the implementation of business continuity procedures.	Administrative change	Updated during Privacy Working Group Offsite; original language modified by HITRUST to focus on privacy implications of business continuity rather than the continuity of the privacy program itself

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
12.b	2	Updated: The Business Continuity Risk Assessment process ~~This process~~ shall identify the critical business processes and integrate the information protection ~~security~~ management requirements of ... The consequences of disasters, security or privacy failures, loss of service, and service availability shall be subject to a business impact analysis Business continuity risk assessments shall … not be limited to the information assets, but shall include the results specific to information security and privacy. It is important to link the different risk aspects together ... The assessment shall … relevant to the organization, including critical resources, impacts of disruptions (including security and privacy concerns), allowable outage times, and recovery priorities.	Administrative change	Updated to reflect changes in 12.b level 1
12.c	Control Name	Added: Developing and Implementing Continuity Plans Including Information Security and Privacy	Administrative change	Updated for consistency with the integration of security and privacy
12.c	1	Updated: The planning process shall focus … of time). The procedures for obtaining necessary electronic PII/PHI ~~covered data~~ during an emergency shall be defined. The services and resources … Developed business continuity plans shall: iv. address maintaining essential missions, business functions and privacy objectives despite an information system disruption, compromise, or failure; … v. address eventual, full information system restoration without deterioration of the security and privacy measures originally planned and implemented; and …	Administrative change	Added during Privacy Working Group Offsite

CSF Control	Control Level	Summary of Changes	Authoritative Source Cross-Reference(s)	Remarks
12.c	2	Updated: The organization shall ensure that the alternate processing site provides information security and privacy measures equivalent to that of the primary site.	Administrative change	Updated to reflect changes in 12.c level 1
12.d	Control Specification	Updated: A single framework … to consistently address information security and privacy requirements …	Administrative change	Updated for consistency with the integration of security and privacy
12.d	1	Updated: The organization shall create at a minimum one business continuity plan. The business continuity plan shall describe … the approach to maintain information or information asset availability, ~~and~~ security and privacy. … The business continuity planning framework shall address ~~the identified~~ information security and privacy requirements …	Administrative change	Updated for consistency with the integration of security and privacy
12.d	2	Updated: The organization shall create at a minimum one business continuity plan. The business continuity plan shall describe … the approach to maintain information or information asset availability, ~~and~~ security and privacy. … A business continuity planning framework shall address ~~the identified~~ information security and privacy requirements …	Administrative change	Updated for consistency with the integration of security and privacy