HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework

In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) as directed in Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The Cybersecurity Framework provides a voluntary, risk-based approach—based on existing standards, guidelines, and practices—to help organizations in any industry to understand, communicate, and manage cybersecurity risks. In the health care space, entities (covered entities and business associates) regulated by the Health Insurance Portability and Accountability Act (HIPAA) must comply with the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI) that they create, receive, maintain, or transmit. This crosswalk document identifies "mappings" between the Cybersecurity Framework and the HIPAA Security Rule.

Organizations that have already aligned their security programs to either the NIST Cybersecurity Framework or the HIPAA Security Rule may find this crosswalk helpful as a starting place to identify potential gaps in their programs. Addressing these gaps can bolster their compliance with the Security Rule and improve their ability to secure ePHI and other critical information and business processes. For example, if a covered entity has an existing security program aligned to the HIPAA Security Rule, the entity can use this mapping document to identify which pieces of the NIST Cybersecurity Framework it is already meeting and which represent new practices to incorporate into its risk management program. This mapping document also allows organizations to communicate activities and outcomes internally and externally regarding their cybersecurity program by utilizing the Cybersecurity Framework as a common language. Finally, the mapping can be easily combined with similar mappings to account for additional organizational considerations (e.g., privacy, regulation and legislation). Additional resources, including a FAQ and overview, are available to assist organizations with the use and implementation of the NIST Cybersecurity Framework.

This crosswalk maps each administrative, physical and technical safeguard standard and implementation specification[1] in the HIPAA Security Rule to a relevant NIST Cybersecurity Framework Subcategory. Due to the granularity of the NIST Cybersecurity

[1] Although all Security Rule administrative, physical, and technical safeguards map to at least one of the NIST Cybersecurity Framework Subcategories, other Security Rule standards, such as specific requirements for documentation and organization, do not. HIPAA covered entities and business associates cannot rely entirely on the crosswalk for compliance with the Security Rule.

Framework's Subcategories, some HIPAA Security Rule requirements may map to more than one Subcategory. Activities to be performed for a particular Subcategory of the NIST Cybersecurity Framework may be more specific and detailed than those performed for the mapped HIPAA Security Rule requirement. However, the HIPAA Security Rule is designed to be flexible, scalable and technology-neutral, which enables it to accommodate integration with frameworks such as the NIST Cybersecurity Framework. A HIPAA covered entity or business associate should be able to assess and implement new and evolving technologies and best practices that it determines would be reasonable and appropriate to ensure the confidentiality, integrity and availability of the ePHI it creates, receives, maintains, or transmits.

The mappings between the Framework subcategories and the HIPAA Security Rule are intended to be an informative reference and do not imply or guarantee compliance with any laws or regulations. Users who have aligned their security program to the NIST Cybersecurity Framework should not assume that by so doing they are in full compliance with the Security Rule. Conversely, the HIPAA Security Rule does not require covered entities to integrate the Cybersecurity Framework into their security management programs. Covered entities and business associates should perform their own security risk analyses to identify and mitigate threats to the ePHI they create, receive, maintain or transmit. Whether starting a new security program or reviewing an existing one, organizations will want to visit OCR's Security Rule compliance guidance; HealthIT.gov for resources on cybersecurity, security risk assessments, security training; as well as the FDA's guidance on cybersecurity for medical devices. To find assistance with the use and implementation of the NIST Cybersecurity Framework, organizations may explore the C-Cubed Voluntary Program and NIST's frequently asked questions.

The table below incorporates mappings of HIPAA Security Rule standards and implementation specifications to applicable NIST Cybersecurity Framework Subcategories. These mappings are included in the "Relevant Control Mappings" column which also includes mappings from other security frameworks. The other columns ("Function", "Category", and "Subcategory") correlate directly to the Function, Category and Subcategory Unique Identifiers defined within the NIST Cybersecurity Framework. Other frameworks included in the mapping to the NIST Cybersecurity Framework include: the Council on Cybersecurity Critical Security Controls (CCS CSC); Control Objectives for Information and Related Technology Edition 5 (COBIT 5); International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 27001; International Society of Automation (ISA) 62443; National Institute of Standards and Technology (NIST) SP 800-53 Rev. 4.

Function	Category	Subcategory	Relevant Control Mappings[2]
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d)
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E)
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d)

[2] Mappings to other standards come from the NIST Cybersecurity Framework, Appendix A and are provided for reference

Function	Category	Subcategory	Relevant Control Mappings[2]
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(ii)(A), 164.308(b), 164.314(a)(1), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 164.316(b)(2)
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)(E)
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b)(1), 164.314

Function	Category	Subcategory	Relevant Control Mappings[2]
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	• COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 • NIST SP 800-53 Rev. 4 CP-2, SA-12 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(4)(ii), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.314, 164.316
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	• COBIT 5 APO02.06, APO03.01 • NIST SP 800-53 Rev. 4 PM-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(4)(ii), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.314, 164.316
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	• COBIT 5 APO02.01, APO02.06, APO03.01 • ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 • NIST SP 800-53 Rev. 4 PM-11, SA-14 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.310(a)(2)(i), 164.316

Function	Category	Subcategory	Relevant Control Mappings[2]
IDENTIFY (ID)		**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established	• ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 • NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(i), 164.308.(a)(7)(ii)(E), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(a)(1), 164.314(b)(2)(i)
		ID.BE-5: Resilience requirements to support delivery of critical services are established	• COBIT 5 DSS04.02 • ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(8), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(b)(2)(i)
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	• COBIT 5 APO13.12 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 • NIST SP 800-53 Rev. 4 PM-1, PS-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.316
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	• COBIT 5 APO13.12 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 • NIST SP 800-53 Rev. 4 PM-1, PS-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b), 164.314

Function	Category	Subcategory	Relevant Control Mappings[2]
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	• COBIT 5 MEA03.01, MEA03.04 • ISA 62443-2-1:2009 4.4.3.7 • ISO/IEC 27001:2013 A.18.1 • NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1) • HIPAA Security Rule 45 C.F.R. §§ 164.306, 164.308, 164.310, 164.312, 164.314, 164.316
		ID.GV-4: Governance and risk management processes address cybersecurity risks	• COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 • NIST SP 800-53 Rev. 4 PM-9, PM-11 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1), 164.308(b)
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	• CCS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	• ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.6.1.4 • NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5 • No direct analog to HIPAA Security Rule[3]
		ID.RA-3: Threats, both internal and external, are identified and documented	• COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.310(a)(1), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(c), 164.312(e), 164.314, 164.316
		ID.RA-4: Potential business impacts and likelihoods are identified	• COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(6), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.316(a)

[3] Even though there is no direct analog, while performing their HIPAA Security Rule required risk analysis, organizations should consider whether participating in cyber-threat sharing programs is reasonable and appropriate to reduce their security risk.

Function	Category	Subcategory	Relevant Control Mappings[2]
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	• COBIT 5 APO12.02 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.316(a)
		ID.RA-6: Risk responses are identified and prioritized	• COBIT 5 APO12.05, APO13.02 • NIST SP 800-53 Rev. 4 PM-4, PM-9 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.314(a)(2)(i)(C), 164.314(b)(2)(iv)
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	• COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • ISA 62443-2-1:2009 4.3.4.2 • NIST SP 800-53 Rev. 4 PM-9 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(B)
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.2.6.5 • NIST SP 800-53 Rev. 4 PM-9 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(B)

Function	Category	Subcategory	Relevant Control Mappings[2]
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	• NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(C),164.308(a)(7)(ii)(E), 164.310(a)(2)(i)
	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• CCS CSC 16 • COBIT 5 DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.3.5.1 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • NIST SP 800-53 Rev. 4 AC-2, IA Family • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.AC-2: Physical access to assets is managed and protected	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 • ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)
		PR.AC-3: Remote access is managed	• COBIT 5 APO13.01, DSS01.04, DSS05.03 • ISA 62443-2-1:2009 4.3.3.6.6 • ISA 62443-3-3:2013 SR 1.13, SR 2.6 • ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	• CCS CSC 12, 15 • ISA 62443-2-1:2009 4.3.3.7.3 • ISA 62443-3-3:2013 SR 2.1 • ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 • NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii)
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	• ISA 62443-2-1:2009 4.3.3.4 • ISA 62443-3-3:2013 SR 3.1, SR 3.8 • ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, SC-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(4)(ii)(B), 164.310(a)(1), 164.310(b), 164.312(a)(1), 164.312(b), 164.312(c), 164.312(e)

Function	Category	Subcategory	Relevant Control Mappings[2]
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	• CCS CSC 9 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2 • NIST SP 800-53 Rev. 4 AT-2, PM-13 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(5)
		PR.AT-2: Privileged users understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D)
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.03, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 PS-7, SA-9 • HIPAA Security Rule 45 C.F.R. §§ 164.308(b), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.AT-4: Senior executives understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, • NIST SP 800-53 Rev. 4 AT-3, PM-13 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D)
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, • NIST SP 800-53 Rev. 4 AT-3, PM-13 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D), 164.530(b)(1)
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	• CCS CSC 17 • COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 • ISA 62443-3-3:2013 SR 3.4, SR 4.1 • ISO/IEC 27001:2013 A.8.2.3 • NIST SP 800-53 Rev. 4 SC-28 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(b)(1), 164.310(d), 164.312(a)(1), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.DS-2: Data-in-transit is protected	• CCS CSC 17 • COBIT 5 APO01.06, DSS06.06 • ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SC-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(b)(1), 164.308(b)(2), 164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii), 164.314(b)(2)(i)
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 • ISA 62443-3-3:2013 SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)
		PR.DS-4: Adequate capacity to ensure availability is maintained	• COBIT 5 APO13.01 • ISA 62443-3-3:2013 SR 7.1, SR 7.2 • ISO/IEC 27001:2013 A.12.3.1 • NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(7), 164.310(a)(2)(i), 164.310(d)(2)(iv), 164.312(a)(2)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.DS-5: Protections against data leaks are implemented	• CCS CSC 17 • COBIT 5 APO01.06 • ISA 62443-3-3:2013 SR 5.2 • ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a), 164.312(e)
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	• ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 • ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SI-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)

Function	Category	Subcategory	Relevant Control Mappings[2]
PROTECT		**PR.DS-7:** The development and testing environment(s) are separate from the production environment	• COBIT 5 BAI07.04 • ISO/IEC 27001:2013 A.12.1.4 • NIST SP 800-53 Rev. 4 CM-2 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(4)[4]
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	• CCS CSC 3, 10 • COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)

[4] Additionally, organizations should consider the HIPAA Privacy Rule "minimum necessary" standard, 45 C.F.R. § 164.502(b), when determining the level of access that is appropriate for development and testing staff.

Function	Category	Subcategory	Relevant Control Mappings[2]
(PR)		**PR.IP-2:** A System Development Life Cycle to manage systems is implemented	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.3 • ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 • NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(i)
		PR.IP-3: Configuration change control processes are in place	• COBIT 5 BAI06.01, BAI01.06 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(8)
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.9 • ISA 62443-3-3:2013 SR 7.3, SR 7.4 • ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 • NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i), 164.310(d)(2)(iv)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)
		PR.IP-6: Data is destroyed according to policy	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4.3.4.4.4 • ISA 62443-3-3:2013 SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • NIST SP 800-53 Rev. 4 MP-6 • HIPAA Security Rule 45 C.F.R. §§ 164.310(d)(2)(i), 164.310(d)(2)(ii)
		PR.IP-7: Protection processes are continuously improved	• COBIT 5 APO11.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 • HIPAA Security Rule 45 C.F.R. §§ 164.306(e), 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	• ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	• COBIT 5 DSS04.03 • ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 • NIST SP 800-53 Rev. 4 CP-2, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6), 164.308(a)(7), 164.310(a)(2)(i), 164.312(a)(2)(ii)
		PR.IP-10: Response and recovery plans are tested	• ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.17.1.3 • NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)(D)
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 • NIST SP 800-53 Rev. 4 PS Family • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(C), 164.308(a)(3)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.IP-12: A vulnerability management plan is developed and implemented	• ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 • NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B)
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4.3.3.3.7 • ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 • NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(A), 164.310(a)(2)(iv)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• COBIT 5 DSS05.04 • ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 • NIST SP 800-53 Rev. 4 MA-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2)(ii), 164.310(d)(2)(iii), 164.312(a), 164.312(a)(2)(ii), 164.312(a)(2)(iv), 164.312(b), 164.312(d), 164.312(e), 164.308(a)(1)(ii)(D)

Function	Category	Subcategory	Relevant Control Mappings[2]
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• CCS CSC 14 • COBIT 5 APO11.04 • ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • NIST SP 800-53 Rev. 4 AU Family • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)
		PR.PT-2: Removable media is protected and its use restricted according to policy	• COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 2.3 • ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b)

Function	Category	Subcategory	Relevant Control Mappings[2]
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	• COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • ISO/IEC 27001:2013 A.9.1.2 • NIST SP 800-53 Rev. 4 AC-3, CM-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)
		PR.PT-4: Communications and control networks are protected	• CCS CSC 7 • COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(a)(1), 164.312(b), 164.312(e)

Function	Category	Subcategory	Relevant Control Mappings[2]
	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	• COBIT 5 DSS03.01 • ISA 62443-2-1:2009 4.4.3.3 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b)
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4 • HIPAA Security Rule 45 C.F.R. § 164.308(6)(i)
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	• ISA 62443-3-3:2013 SR 6.1 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(8), 164.310(d)(2)(iii), 164.312(b), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
		DE.AE-4: Impact of events is determined	• COBIT 5 APO12.06 • NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		DE.AE-5: Incident alert thresholds are established	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.2.3.10 • NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(i)
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• CCS CSC 14, 16 • COBIT 5 DSS05.07 • ISA 62443-3-3:2013 SR 6.2 • NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.312(b), 164.312(e)(2)(i)
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	• ISA 62443-2-1:2009 4.3.3.3.8 • NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20 • HIPAA Security Rule 45 C.F.R. §§ 164.310(a)(2)(ii), 164.310(a)(2)(iii)

Function	Category	Subcategory	Relevant Control Mappings[2]
DETECT (DE)		**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events	• ISA 62443-3-3:2013 SR 6.2 • ISO/IEC 27001:2013 A.12.4.1 • NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)
		DE.CM-4: Malicious code is detected	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.3.4.3.8 • ISA 62443-3-3:2013 SR 3.2 • ISO/IEC 27001:2013 A.12.2.1 • NIST SP 800-53 Rev. 4 SI-3 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)
		DE.CM-5: Unauthorized mobile code is detected	• ISA 62443-3-3:2013 SR 2.4 • ISO/IEC 27001:2013 A.12.5.1 • NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	• COBIT 5 APO07.06 • ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(1)(ii)(D)

Function	Category	Subcategory	Relevant Control Mappings[2]
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	• NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)
		DE.CM-8: Vulnerability scans are performed	• COBIT 5 BAI03.10 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-5 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(8)
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.4.3.1 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(a)(2)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		DE.DP-2: Detection activities comply with all applicable requirements	• ISA 62443-2-1:2009 4.4.3.2 • ISO/IEC 27001:2013 A.18.1.4 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(8)
		DE.DP-3: Detection processes are tested	• COBIT 5 APO13.02 • ISA 62443-2-1:2009 4.4.3.2 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.14.2.8 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 • HIPAA Security Rule 45 C.F.R. § 164.306(e)
		DE.DP-4: Event detection information is communicated to appropriate parties	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.4.5.9 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
		DE.DP-5: Detection processes are continuously improved	• COBIT 5 APO11.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 • HIPAA Security Rule 45 C.F.R. §§ 164.306(e), 164.308(a)(8)

Function	Category	Subcategory	Relevant Control Mappings[2]
	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	• COBIT 5 BAI01.10 • CCS CSC 18 • ISA 62443-2-1:2009 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.312(a)(2)(ii)
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	• ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 • NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(2), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.308(a)(6)(i), 164.312(a)(2)(ii)
		RS.CO-2: Events are reported consistent with established criteria	• ISA 62443-2-1:2009 4.3.4.5.5 • ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 • NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)

Function	Category	Subcategory	Relevant Control Mappings[2]
		RS.CO-3: Information is shared consistent with response plans	• ISA 62443-2-1:2009 4.3.4.5.2 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.314(a)(2)(i)(C)
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• ISA 62443-2-1:2009 4.3.4.5.5 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6), 164.308(a)(7), 164.310(a)(2)(i), 164.312(a)(2)(ii)
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• NIST SP 800-53 Rev. 4 PM-15, SI-5 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)

Function	Category	Subcategory	Relevant Control Mappings[2]
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	• COBIT 5 DSS02.07 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.312(b)
		RS.AN-2: The impact of the incident is understood	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 CP-2, IR-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(E)
		RS.AN-3: Forensics are performed	• ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • ISO/IEC 27001:2013 A.16.1.7 • NIST SP 800-53 Rev. 4 AU-7, IR-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)
		RS.AN-4: Incidents are categorized consistent with response plans	• ISA 62443-2-1:2009 4.3.4.5.6 • ISO/IEC 27001:2013 A.16.1.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)

Function	Category	Subcategory	Relevant Control Mappings[2]
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	• ISA 62443-2-1:2009 4.3.4.5.6 • ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
		RS.MI-2: Incidents are mitigated	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 • ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(ii)
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	• ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(6)(ii)
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	• COBIT 5 BAI01.13 • ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii))
		RS.IM-2: Response strategies are updated	• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8)
	Recovery Planning (RC.RP): Recovery	**RC.RP-1:** Recovery	• CCS CSC 8

Function	Category	Subcategory	Relevant Control Mappings[2]
RECOVER (RC)	processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	plan is executed during or after an event	• COBIT 5 DSS02.05, DSS03.04 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7), 164.310(a)(2)(i)
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	• COBIT 5 BAI05.07 • ISA 62443-2-1:2009 4.4.3.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)
		RC.IM-2: Recovery strategies are updated	• COBIT 5 BAI07.08 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(7)(ii)(D), 164.308(a)(8)
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and	**RC.CO-1:** Public relations are managed	• COBIT 5 EDM03.02 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(i)[5]
		RC.CO-2: Reputation after an event is repaired	• COBIT 5 EDM03.02 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(6)(i) [5]

[5] Although public relations management and reputation repair are not specifically required by the HIPAA Security Rule's Security Incident Procedures standard (45 C.F.R. § 164.308(a)(6)(i)), HIPAA covered entities and business associates may implement such procedures as components of their compliance activities.

Function	Category	Subcategory	Relevant Control Mappings[2]
	vendors.	**RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams	• NIST SP 800-53 Rev. 4 CP-2, IR-4 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(6)(ii), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.310(a)(2)(i), 164.314(a)(2)(i)(C)