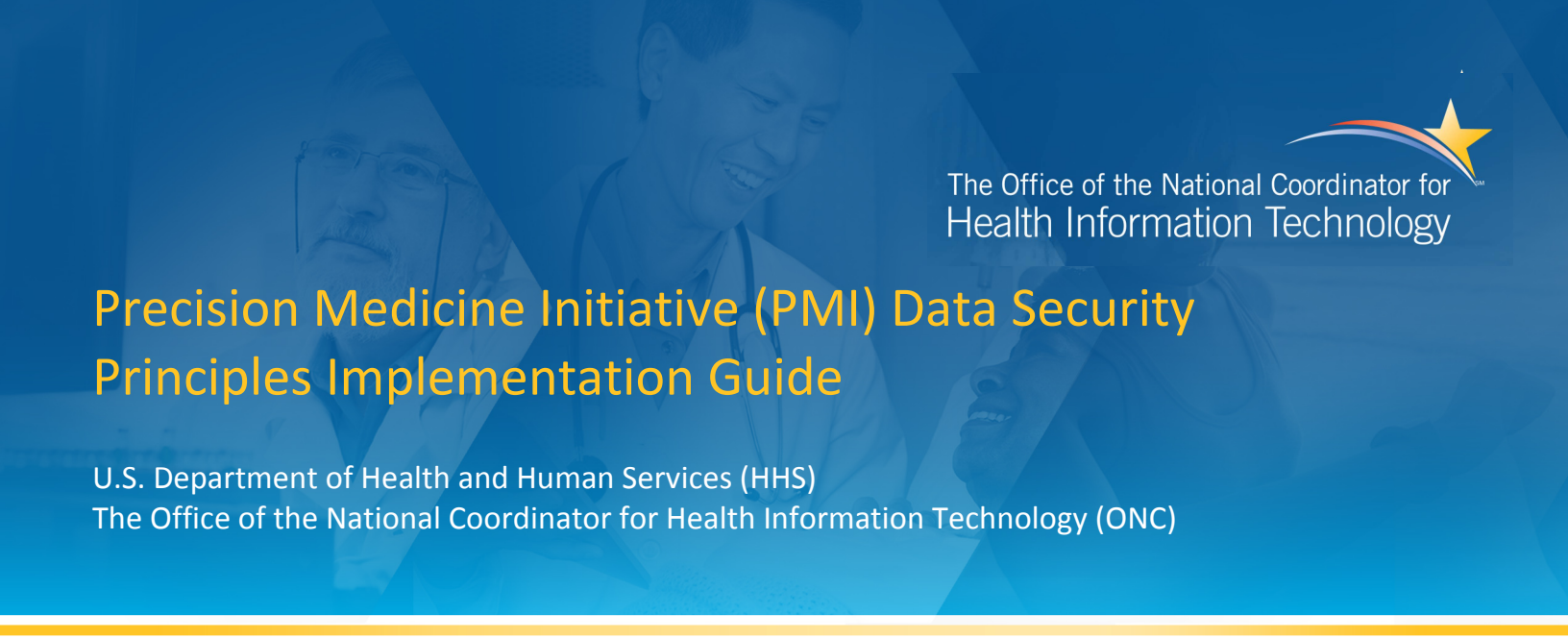

The Office of the National Coordinator for Health Information Technology

Precision Medicine Initiative (PMI) Data Security Principles Implementation Guide

U.S. Department of Health and Human Services (HHS)
The Office of the National Coordinator for Health Information Technology (ONC)

Disclaimer

The Precision Medicine Initiative Data Security Principles Implementation Guide *at HealthIT.gov is provided for informational purposes only. Use of this guide is neither required by nor guarantees compliance with federal, state or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations. The* Precision Medicine Initiative Data Security Principles Implementation Guide *is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. For more information about the HIPAA Privacy and Security Rules, please visit the* HHS Office for Civil Rights Health Information Privacy website.

NOTE: The NIST Standards and Guidelines provided in this guide are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management.

This guide is not intended to serve as legal advice or as recommendations based on an organization's, provider's, or security professional's specific circumstances. We encourage organizations, providers, and security professionals to seek expert advice when evaluating the use of this guide

Acknowledgments

We thank the individuals who contributed to development of the Precision Medicine Initiative Data Security Principles Implementation Guide, namely, Jeremy Maxwell at the Office of the National Coordinator for Health Information Technology (ONC), Nick Heesters at the HHS Office for Civil Rights (OCR), and Kevin Stine and Matthew Barrett at the National Institute of Standards and Technology (NIST).

Contents

Figures

Tables

1. Project Charter & How to Use this Document

Launched in 2015, the Precision Medicine Initiative (PMI)[1] aims to move away from the "one-size-fits-all" approach to health care delivery and to instead tailor treatment and prevention strategies to people's unique characteristics, including environment, lifestyle, and genes. The White House released a trust framework for PMI to ensure that PMI data is appropriately secured and protected. This framework includes principles for both privacy[2] and data security.[3]

Additionally, in February 2016, the White House announced that the Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the National Institute of Standards and Technology (NIST) and the Office for Civil Rights (OCR), would develop a precision medicine-specific guide to the NIST Cybersecurity Framework[4] by December 2016. This guide, called the "Precision Medicine Initiative Data Security Principles Implementation Guide," was developed to provide best practices in security and data management for precision medicine.

The guide will assist organizations that use patient data for research by helping them:

- Execute the principles laid out in the White House's "Precision Medicine Initiative: Data Security Policy Principles and Framework" document;
- Ensure that they maintain a strong security strategy with respect to the data collected and generated about precision medicine participants; and
- Prioritize participant trust.

This document builds on the PMI Data Security Policy Principles and Framework. The Data Security Policy Principles provide a broad framework for protecting PMI participants' data based on the NIST Cybersecurity Framework. The PMI Data Security Principles Implementation Guide outlines how the Data Security Policy Principles would apply to an example PMI use case.

The use case outlined in this document (Section 2) is a fictional use case based on existing ONC patient-centered outcomes research work. The guide then demonstrates how a fictional Chief Information Security Officer (CISO) named Sally could perform a security risk assessment on the systems described in the use case (Section 3). The guide concludes by describing steps Sally can take to address the risks she identified in her security risk assessment (Sections 4 and 5).

The guidance provided by this document is non-prescriptive in order to be flexible and scalable as the security threat landscape is constantly evolving. The list of security risks identified for the sample PMI use case (see Appendix A) is for illustrative purposes only and does not represent a complete, enterprise-wide identification and assessment of the risks to PMI data for an organization.

---

[1] Learn more about PMI at https://www.whitehouse.gov/precision-medicine.

[2] Access "Precision Medicine Initiative: Privacy and Trust Principles" at https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/PMI_Security_Principles_and_Framework_FINAL_022516.pdf.

[3] Access "Precision Medicine Initiative: Data Security Policy Principles and Framework" at https://obamawhitehouse.archives.gov/sites/obamawhitehouse.archives.gov/files/documents/PMI_Security_Principles_Framework_v2.pdf .

[4] The NIST Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines, and practices, that critical infrastructure organizations can use to better manage and reduce cybersecurity risk. The framework also fosters risk and cybersecurity management communications amongst both internal and external organizational stakeholders. For more information, visit https://www.nist.gov/cyberframework.

In addition, some organizations that are using PMI data for research may be Health Insurance Portability and Accountability Act (HIPAA) covered entities, HIPAA business associates, or not covered by HIPAA at all. Following this guidance does not guarantee or imply compliance with the HIPAA Privacy, Security, and Breach Notification regulations (the HIPAA Rules), as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), or any other federal or state laws.

Organizations should perform their own security risk assessments to accurately and thoroughly identify and assess the risks to the confidentiality, integrity, and availability to PMI data processed, stored, or transmitted throughout their enterprises. Furthermore, organizations should implement security controls sufficient to reduce these risks to a reasonable and appropriate level.

HIPAA covered entities and business associates who are also using PMI data for research can find more information about how the PMI Data Security Policy Principles align with the HIPAA Security Rule in Appendix B. More information on health care privacy and security can be found at healthIT.gov, hhs.gov/ocr, and csrc.nist.gov.

1.1. Intended Audience

This document is intended for organizations that use patient data for research, including precision medicine research. These may include:

- Organizations that are participating in the PMI or the National Institutes of Health (NIH) All of UsSM Research Program,[5]
- Organizations that are using PMI data for research outside these federal programs, or
- Contractors supporting organizations using PMI data for research.

Security officers, information technology (IT) staff, and management staff can use this document to help them identify the kinds of risks and topics they should consider when performing their own security risk assessments.

2. Use Case

This document examines and applies the PMI Data Security Policy Principles and Framework to a PMI-related use case. The use case is based on use cases developed as part of the Patient-Centered Outcomes Research (PCOR) Privacy and Security Research Scenario Initiative and Legal Analysis and Ethics Framework project[6] (or PCOR Research Scenario Project, for short). The PCOR Research Scenario Project seeks to determine how electronic health information derived from a wide variety of data sources can be used for PCOR consistent with ethics principles and legal and regulatory requirements related to patient consent, privacy, and autonomy.

The use cases developed by the PCOR Research Scenario Project are policy-oriented use cases, meaning they are oriented towards an organization's security policies. To illustrate the Data Security Principles,

[5] Learn more at the NIH *All of Us* Research Program website, available at https://www.nih.gov/precision-medicine-initiative-cohort-program.

[6] Learn more about the PCOR Research Scenario Project at http://confluence.sifframework.org/display/PSRSI/PCOR+Privacy+and+Security+Research+Scenario+Initiative+and+Legal+Analysis+and+Ethics+Framework+Development+Home.

the use cases developed by the PCOR Research Scenario Project have been augmented with technical details (see Figure 1).

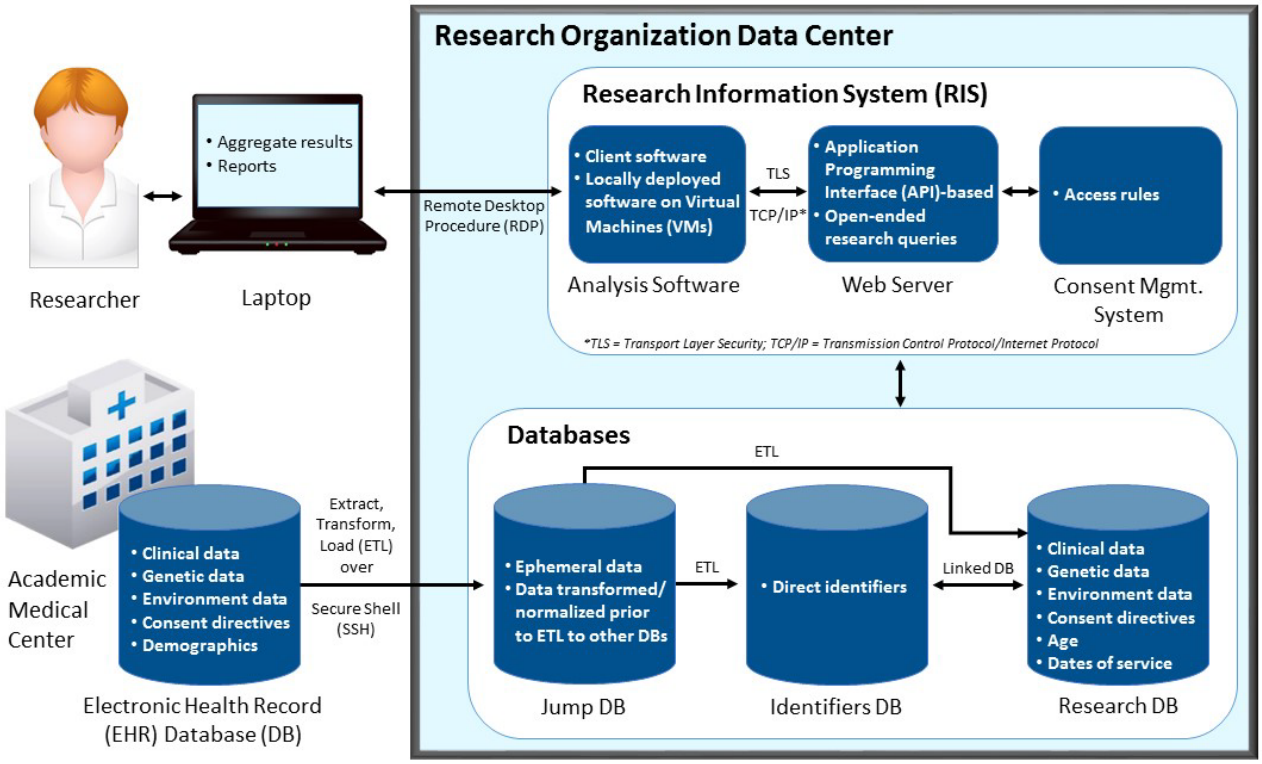

Figure 1. Technical Use Case Elaboration

2.1. Use Case Narrative

Alice works for Acme Research Organization (Acme) as a researcher that is performing an Institutional Review Board (IRB)-approved research study in partnership with University Academic Medical Center. To perform this research, Alice uses her laptop to connect to a Research Information System (RIS). She connects remotely from her laptop to a Virtual Machine (VM) that contains analysis software used as part of the research study. Research participants' information remains on the VM — only aggregate results that contain no direct patient identifiers and reports are downloaded to the researcher's laptop.

Acme stores research data in two databases — an identifiers database (Identifiers DB) and a research database (Research DB). The Identifiers DB contains direct identifiers such as participant name, mailing address, date of birth, and email address. The Research DB contains participant data such as clinical data, genetic and biospecimen derived data, participant age, and dates of service. The two databases are linked together via software process so that joined queries can be made across both databases.

The Identifiers DB and Research DB are populated with data under IRB approval from University Academic Medical Center. All patient data has either been supplied with the participants' consent or with a waiver of consent under IRB approval. Data from the Academic Medical Center's electronic health record (EHR) system is transferred via an Extract, Transform, Load (ETL) process over an open source Secure Shell (SSH) tunnel. Once transferred to a server hosting a temporary database (Jump DB), the data is normalized and transferred to the Identifiers and Research DBs.

The analysis software on the VM connects to a web server using an application programming interface (API) over the Transport Layer Security (TLS) protocol. The web server communicates with databases containing research data and returns results of queries submitted by Alice.

The web server employs a consent management system to determine if the data should be available to respond to Alice's query. The consent management system uses role-based access control when making access decisions.

Sally recently joined Acme as the CISO. Sally's job is to ensure the confidentiality, integrity, and availability of Acme's research data and systems.

2.2. Use Case Assumptions & Notes

- In the use case, specific vendors or technology providers are not identified.
- In the use case, Acme is neither a HIPAA covered entity nor a business associate. As such, Acme is not regulated under the HIPAA Rules for purposes of the use case.
- While the technical elaboration illustrates a centralized data warehouse architecture, this is not an endorsement of one architecture over another. Multiple architecture designs are valid solutions for PMI use cases.
- The consent management system is collocated with the RIS and has the same security requirements.
- The security risk assessment described in this document is for illustrative purposes only, limited in scope of the sample PMI use case, and is not representative of an enterprise-wide security risk assessment.

3. Security Risk Assessment

As the newly hired CISO, one of Sally's first tasks is to perform a security risk assessment to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of Acme's PMI data and systems. Sally employs the PMI Data Security Policy Principles and Framework to guide her risk assessment. Additionally, she leverages the NIST standards and guidelines that have been outlined by the Federal Information Security Management Act (FISMA) in conjunction with other NIST standards and guidelines. Her NIST reference for risk assessments is the NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments.[7]

3.1. Preparing for the Security Risk Assessment

To prepare for a security risk assessment, Sally must:

1. Identify the purpose of the assessment,
2. Determine the scope of the assessment as well as any assumptions and constraints,
3. Identify what sources of information she will use, and
4. Determine the risk model and analytic approach.

3.1.1. Identify the Purpose of the Security Risk Assessment

Sally is using the security risk assessment to better understand the security posture of the organization. During the process, she will identify threats to the confidentiality, integrity, and availability of PMI data

[7] The NIST Special Publication 800-30 Revision 1 is available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

and systems, as well as assess the effectiveness of existing security controls that address identified risks. Any unaddressed threats will be assessed for the risk they pose to the organization.

Sally recognizes that her work does not end when the security risk assessment is completed. She will have to develop a plan for responding to any unacceptable risks, as well as for conducting periodic reassessments for changed circumstances. Operational and environmental changes that affect the security of PMI data will occur over time; she will have to work with the organization's management and IT staff to understand the organization's plans for upgrades and other changes which can affect PMI security. Doing so will allow her to revisit the security risk assessment and assess the risks these changes pose to PMI data before they are implemented.

Cybersecurity threats also evolve over time. Once she completes the security risk assessment, Sally plans to seek out Information Sharing and Analysis Organizations (ISAOs)[8] for her organization to participate in. Participating in an ISAO allows her to keep up-to-date on evolving security threats.

3.1.2. Determine the Scope of the Security Risk Assessment

For the purposes of this document, Sally's task is to perform the security risk assessment only on the PMI data and related systems, including the flow of PMI data into, out of, and among the organization's related systems. A complete security risk assessment for Acme as a whole would have to consider Acme's entire enterprise. Acme and Sally must also have plans in place, outside of the exercise in this document, to address any necessary improvements to preserve the confidentiality, integrity, and availability of Acme's enterprise systems; that analysis, however, is beyond the scope of this use case. Sally plans on conducting further security risk assessments that cover these important areas.

3.1.3. Identify Sources of Information

To perform the security risk assessment, Sally relies on her professional experience, interviews with key organizational stakeholders and subject matter experts, manual review of the deployed systems, and automated tools such as vulnerability scanners. To keep up-to-date with the latest security threats, Sally maintains membership in related professional organizations, attends training webinars and security conferences, and keeps up-to-date with security news.

3.1.4. Determine the Risk Model and Analytic Approach

She plans to align her security risk assessment with the PMI Data Security Policy Principles and Framework. Because the Principles are aligned to the NIST Cybersecurity Framework, this will help Sally organize her risk assessment and communicate it to others throughout the organization. Once she identifies security risks, she plans on ranking them by severity so she knows which risks to prioritize for remediation. To rank security risks, she plans on using the Common Vulnerability Scoring System version 3 (CVSSv3).[9]

In CVSS, security risks are ranked along three dimensions: a base score, a temporal score, and an environmental score. The base score captures the characteristics of the vulnerability that are constant over time and across environments. This score is modified by the temporal and environmental score. The temporal score captures how risks may change over time. For example, vulnerabilities may initially be hard to exploit and thus have a low risk score, but later may be included in an easy-to-use exploit software which raises the score. The environmental score captures characteristics that are unique to the

[8] More information about ISAOs is available through ONC at https://www.healthit.gov/newsroom/onc-funding-cyber-threat-information-sharing-health-care-and-public-health-hph-sector.
[9] The CVSSv3 is available at https://nvd.nist.gov/CVSS/v3-calculator.

user's environment. Even though this scoring system is typically used for ranking technical vulnerabilities (such as an unpatched system), Sally believes that using the same scoring rubric for all security risks helps prioritize those risks.

3.2. Performing the Security Risk Assessment

3.2.1. Identify Assets

Assets are defined in NIST Special Publication 800-30 Revision 1:[10]

> *The term* organizational assets *can have a very wide scope of applicability to include, for example, high-impact programs, physical plant, mission-critical information systems, personnel, equipment, or a logically related group of systems. More broadly, organizational assets represent any resource or set of resources which the organization values, including intangible assets such as image or reputation.*

Sally works with researchers, IT staff, and management to identify systems and assets that process, store, or transmit PMI data for Acme. These assets include:

- Researcher laptops
- Patient data, particularly direct identifiers
- Web servers, computing, and networking resources
- User credentials such as passwords
- Organizational reputation
- Public trust and confidence

It is clear why some of these assets are valued, e.g., if information systems or data become compromised, the research organization's mission is impacted. Public trust and confidence is important because PMI relies on individuals consenting for their information to be included in the research dataset — if individuals lose confidence in research organizations' ability to protect their data, the amount and quality of available research data will diminish.

3.2.2. Identify Threats and Calculate Risks

In this step of the security risk assessment, Sally identifies and characterizes threat sources of concern, including capability, intent, and targeting characteristics for adversarial threats (such as a hacker gaining fraudulent access to PMI systems), and range of effects for non-adversarial threats (such as an employee losing a laptop). To help her organize the security risk assessment, Sally uses a spreadsheet to track threats and calculate risk scores (see Appendix A). To brainstorm threats to PMI data and systems, Sally relies on her professional experience, industry news, professional associations, information from the Common Vulnerabilities and Exposures (CVE) dictionary,[11] and common vulnerability lists such as the Open Web Application Security Project (OWASP) Top 10 Project[12] and the SANS Top 25 Most Dangerous Software Errors.[13]

[10] NIST Special Publication 800-30 Revision 1 is available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.
[11] The CVE dictionary is available at http://cve.mitre.org/.
[12] More information about the OWASP Top 10 Project is available at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.
[13] Learn more about the SANS Top 25 Most Dangerous Software Errors at http://www.sans.org/top25-software-errors/.

Sally first documents threats to the confidentiality, integrity, and availability of Acme's PMI data. She groups these threats according to each PMI Data Security Principle. For each threat, she then documents mitigating controls that are already in place at Acme. She then identifies any gaps in these controls, that is, unmitigated or residual risks to Acme's systems or PMI data. When she is done with the risk assessment, the list of gaps will be used in the development of a remediation plan. Finally, she uses the CVSSv3 scoring system to determine a risk score for the threat (see Table 1 for examples).

PMI Data Security Principle	Threats	Mitigating Controls	Gaps	CVSSv3 Base Score Metrics	CVSSv3 Temp-oral Score Metrics	CVSSv3 Env Score Metrics	CVSSv3 Overall Score
Credentials	1. Hacker guesses weak user password	1. Systems require complex passwords	1. Complex passwords are not strong in practice	7.3	6.9	7.6	7.3
Credentials	2. User selects easily guessed password	2. None known	2. Complex passwords are difficult to remember	7.3	7.1	7.8	7.4
Encryption	1. Research data is compromised on lost/stolen laptop/device	1. Users are only supposed to have aggregate results on laptop/ devices	1. Users may ignore policy and store identifiable data on laptop/devices	6.1	6.1	6.8	6.3
Encryption	2. Hacker exfiltrates data from the database after gaining fraudulent access	2. Direct identifiers are stored separately from research data	2. The compromise of directed Identifiers DB is still a data breach	8.1	8.1	8.6	8.3

Table 1. Identifying Threats and Calculating Risks

3.3. Discovering New Information During the Security Risk Assessment

Oftentimes during the course of a security risk assessment, new information may surface. During the course of her security risk assessment, Sally discovers that the RIS used by Acme is not the first version of the system. Acme maintains a legacy version of the RIS. The legacy system contains PMI data held in read-only mode to allow referencing of data used in prior studies. The legacy system is no longer supported by the RIS vendor and is deployed on legacy operating systems that no longer receive security updates.

Ideally, legacy systems and servers that no longer receive security updates should be migrated to modern systems. However, this is not always possible. For example, the data formats used by the legacy RIS are different than the current RIS, and performing a custom data mapping and migration to move the data onto a modern platform would be cost-prohibitive. Thus, Acme business executives determine

that the legacy RIS must remain operational for the foreseeable future, and Sally must develop a plan to secure the legacy systems (see Section 4.4.4).

3.4. Prioritizing Risks

Not all security risks are created equal. Oftentimes, risks are compared using their likelihood (the chance that the threat will be actualized) and their impact (the business impact of the threat becoming actualized). During her security risk assessment, Sally uses the CVSSv3 scoring system to determine relative scores for each risk. These risk scores are not an absolute rule, but rather a guideline regarding which risks the organization may need to address first. Additional considerations can influence priorities such as time to address the risk, cost of mitigating security controls, organizational risk tolerance, and the presence of compensating controls. For additional information on risk prioritization, see Appendix J of NIST Special Publication 800-30 Revision 1.[14]

4. Addressing of Threats Identified During the Security Risk Assessment

Once security risks have been identified and prioritized, the organization performing the security risk assessment can develop plans to mitigate the security risks. Not all security risks can be addressed. Some risks are unknown, such as "zero day" vulnerabilities.[15] Other times, due to limited time and resources, organizations may decide to accept low-severity security risks. Different organizations will have different levels of risk they will accept; this is called their "risk tolerance" or "risk appetite." An organization's risk tolerance may be influenced by the requirements of their research contracts and funding opportunities.

Organizations can choose multiple strategies for addressing identified risks,[16] such as:

- *Implementing controls that reduce the risk.* For example, antivirus and antimalware solutions directly reduce the risk of malicious software.
- *Implementing compensating controls.* For example, patching legacy systems is the ideal, but legacy systems may not have security patches available. Isolating legacy systems on a separate network without access to the Internet is a compensating control that reduces the risk that unpatched systems will be breached.
- *Ensuring risks are addressed in contracts*. Risks may arise because of relationships between Acme and consultants, suppliers, or other research institutions. All of these relationships are documented in contracts. The relevant contracts need to specifically address privacy and security issues, including financial responsibility for privacy and security through liability terms and indemnification clauses.
- *Purchasing cyber insurance to cover the risk.* Cyber insurance can blunt the impact that security risks have on a business. Organizations should carefully review cyber insurance policies to understand the scope of the policies and ensure that identified risks are actually covered.
- *Destroying the data.* Data that has been properly destroyed[17] is no longer at risk of being improperly accessed or modified. Organizations should regularly review their document and

[14] NIST Special Publication 800-30 Revision 1 is available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.
[15] A "zero day" vulnerability is a software vulnerability that is not known until it is exploited by hackers.
[16] For more risk mitigation strategies, see Appendix H of NIST Special Publication 800-30 Revision 1, available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.
[17] For more information on proper media sanitization, see NIST Special Publication 800-88 Revision 1, available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

data retention policies to ensure that old data is not being held for longer than needed by the business. Organizations may also need to consult state law, as data retention policies often vary by state.

- *Accepting the risk*. Not all risks can be eliminated — organizations should determine the level of risk with which they're comfortable.

After concluding the security risk assessment, Sally identifies several key themes for which she needs to develop a plan to address. This section does not discuss every security risk that Sally may have to address. Many of those risks are outlined in Appendix A. This section only highlights the critical and high severity risks that Sally identified during her security risk assessment.

4.1. Identity Management

Identity management is an essential building block for system security. Identity management controls ensure that users have access to the right information, at the right time, for the right reasons. Sally identified identity management risks during the security risk assessment, such as the risk that a hacker could gain fraudulent access using a legitimate account (see Risks 5-8 in Appendix A). Once the hacker gains system access, he or she can steal PMI research data to perform identity theft or can install ransomware or other malicious software.

To guide her in determining the appropriate level of identity management for researchers, Sally relies upon the draft NIST Special Publication 800-63A: Digital Authentication Guideline.[18] Organizations such as Acme should contemplate several key aspects of their identity management strategy, including identity proofing, credentialing, authentication, and de-provisioning.

4.1.1. Identity Proofing

Identity proofing is the process of providing sufficient documentation to prove a person is who he/she claims to be. Identity proofing occurs in everyday life, such as when an individual provides a government-issued identification, proof of residence, and Social Security Number while seeking a loan or employment. In the digital world, once an individual is identity-proofed, a digital identity is created and associated with that physical person. In the PMI use case, the researcher Alice is the individual who needs to be identity-proofed by Acme.

Currently, Acme's research systems do not allow for research participants (i.e., the individuals whose data is in the systems) to directly access the system. Therefore, Sally does not have to address risks arising from identity-proofing research participants. Sally does, however, have to contemplate risks from the identity proofing of researchers such as Alice. Researchers have access to many records at a time, meaning their accounts require more robust identity management processes than those accounts that can only access a single record (such as a participant accessing his/her own data).

Identity proofing processes should establish identity to a level of assurance appropriate to the service being delivered and the sensitive nature of the data. To address identity proofing risks in her organization, Sally determines, as a result of the risk assessment, that Acme's researchers (who are all employees of Acme) should be required to be identity-proofed in-person. Identity proofing for Acme employees occurs during the employee onboarding process, where the researcher supplies government identification, Social Security Number, and proof of residence. Acme does not support a virtual identity proofing process, as the organization requires all new employees to attend on-site training and

[18] NIST Special Publication 800-63A is available at https://pages.nist.gov/800-63-3/sp800-63a.html.

orientation, even if those employees will be full-time teleworkers. During the identity proofing process, Acme Human Resources (HR) staff members validate that all evidence supplied is valid (correct) and genuine (not counterfeit or misappropriated).

4.1.2. Credentialing

Credentials are security tokens or objects that provide proof of identity and entitle the user to the privileges associated with that identity. Credentials are assigned to a user upon successful identity proofing and are used to prove a user's identity during the authentication process (see Section 4.1.3). Credentials commonly include username and password, certificates, biometrics such as a thumb swipe, or a physical token such as a smart card. Ideally, the credential should have measures that prevent the credential from being guessed, counterfeited, or tampered with. Once assigned, credentials should be protected with controls such as encryption or hashing (see Section 4.3.2).

At Acme, researchers have access to many records at a time. To prevent risks of fraudulent access, Sally determines, as a result of the risk assessment, that Acme should assign each researcher two credentials. This enables multi-factor authentication as discussed in the next section. Each Acme researcher is assigned a username and password (the first credential). Additionally, each researcher is enrolled in a one-time password program (the second credential). When the researcher attempts to login to the RIS, a code is sent to his/her smartphone through a one-time password mobile application (app). Acme employs these controls for user accounts that have access to many PMI records.

Even though it is out of scope for this use case, Sally's risk assessment could indicate a lower risk for patient accounts that have access to a single PMI record, such as an individual participant requesting access to his/her own PMI data. With a lower risk level, Sally could determine that single-factor authentication is reasonable and appropriate for user accounts that have access to only a single PMI record.

4.1.3. Authentication & Authorization

Authentication is the process of verifying the identity of the user who is attempting to access an information system. To authenticate to a system, the user presents his/her credentials and the system verifies the authenticity of those credentials. For example, the user may provide a username and password. For successful authentication to occur, the system would then verify that the information matches with the username and password stored in the system.

As discussed in the previous section, each Acme researcher is granted two credentials — a username and password as well as a one-time password mobile application (app) for his/her smartphone. For our use case, passwords alone do not provide enough protection against fraudulent use of researcher accounts with access to many PMI records; thus, Acme requires the use of multi-factor authentication.

While authentication does nothing more than link a person to an electronic identity, authorization is the process of verifying that a user has permissions to perform the requested actions within the system. Typically, when users are provisioned with an identity in the system, they are assigned permissions based on their role in the organization (also called role-based access control). Acme employs a consent management system that checks a user's data query against a set of consent rules to determine if the user can access the requested dataset. However, Acme resides in a state that has specific laws governing access to the health data of individuals with impaired decision-making capacity who cannot provide consent for research purposes due to a particular mental condition or disability. According to the state's law, a Legal Authorized Representative (LAR) may provide proxy consent, unless the individual's capacity

to consent changes. This issue would require Sally to review the rules in the consent management system to ensure that the state's laws are followed.

4.1.4. De-Provisioning

Users regularly change roles within Acme or leave the organization altogether. De-provisioning is the process of revoking user permissions to access the system when the user's role changes. When a user is de-provisioned, his/her identity remains in the system, but his/her credentials and permissions are revoked. The user identity must remain in the system for auditing purposes, for example. If the user identity were removed, another user could be assigned that identity. A security officer reviewing the audit trail would not know which individual performed each action.

Acme has automated methods of de-provisioning users in situations such as when they leave the organization. Additionally, Sally implements a regular review process to periodically check that each user's access is appropriate for his/her current role.

4.2. De-Identification

As discussed in Section 2.1, data stored in Acme's RIS is segmented into two data warehouses. The Identifiers DB contains direct identifiers such as participant name, mailing address, date of birth, and email address. The Research DB contains participant data such as clinical data, genetic and biospecimen derived data, participant age, and dates of service. In this use case, Acme is not a HIPAA covered entity or business associate, and the research data is not considered electronic Protected Health Information (ePHI) covered by HIPAA; however, Acme still employs the de-identification standards under the HIPAA Privacy Rule as a best practice for purposes of releasing datasets to users. Furthermore, the Common Rule, which regulates federally supported human subjects research, states that information is identifiable if "the identity of the individual is or may be readily ascertained by the [researcher] or associated with the information."[19] However, the Common Rule does not apply in cases where the information is not identifiable.

Under the HIPAA Privacy Rule, data may be de-identified using two methods:[20]

- The Expert Determination Method – This method occurs when a statistical or scientific expert reviews the dataset and determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information.
- The Safe Harbor Method – This method occurs when data holders remove 18 data elements specified by the HIPAA Privacy Rule. These data elements include individual names, addresses, contact information, and dates of service.

Organizations, particularly HIPAA covered entities and business associates, should consider de-identification controls in their security risk assessments. Because de-identified data is no longer considered identifiable, de-identified data may have reduced security requirements compared to identifiable data. De-identified data may still be subject to other federal or state laws. To maintain the data's status as de-identified, the data cannot be rendered partially or wholly identifiable by the addition of data from other sources.

[19] 45 Code of Federal Regulations (CFR) § 46.102(f) (2015).
[20] For more information on HIPAA de-identification, visit http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/.

In addition, another reason to evaluate de-identification as a security technique is that research, like many other uses of identifiable data, is subject to the concept of necessity: researchers should not have access to data they do not need to test their hypothesis. This can be solved with de-identification if in some circumstances identifiers are not needed to test the research hypothesis.

Under the HIPAA Privacy Rule, the data contained within the research database would not be considered de-identified data under the Safe Harbor method. The dataset within the research database contains dates of service — an indirect identifier that must be removed to satisfy Safe Harbor de-identification. Under the Safe Harbor method, de-identification is binary — either all 18 data elements are removed and it is considered de-identified, or some of the 18 data elements are present and it is considered ePHI (see Appendix C).

Therefore, Acme uses the Expert Determination method to determine that the risk of re-identification is low enough to meet the HIPAA standard. To meet the Expert Determination method, Acme uses an independent statistical or scientific expert to determine the risk is low for a *given dataset* based on data replicability, availability of other datasets, distinguishability of the data elements, availability of other datasets,[21] and other factors. However, because researchers add and remove data from the research database on a regular basis, Acme cannot rely on a one-time, blanket determination that the dataset is always de-identified; Acme must have its expert continually assess new or changed datasets for de-identification purposes.

4.3. Encryption

A risk Sally identified during the security risk assessment is the need to protect the confidentiality of PMI data (see Risks 11-13 in Appendix A). Encryption is a cryptographic process of encoding data so that unauthorized parties cannot view the data. An encryption key is used in an encryption process to render data unusable, unreadable, and indecipherable. A user needs the encryption key to decrypt the data to make it readable again. Encryption is an important security control, as an accidental exposure of data that has been properly encrypted is not considered a breach under many breach notification laws.

When encryption is not used, a relatively common security event such as a lost laptop or mobile phone can become a costly data breach. While not using encryption does not itself create additional security threats, choosing not to encrypt data magnifies the impact of other security risks. Take health care as an example, where at least 29% of breaches affecting 500 or more individuals from September 2009 through September 2016 could have been prevented had the HIPAA covered entity or business associate properly implemented encryption.[22] Simply encrypting the data is not enough, however. If the encryption key is compromised along with the encrypted data, then there is no guarantee that the data is protected.

Sally identifies several security risks that can be addressed by encryption controls. Encryption controls to address the risks Sally identified can be grouped into two categories: encryption to protect user devices, and securing of the credentials used to unlock that encryption. Encryption is an important security control that can be applied to other contexts, such as encrypting data in transit. Acme already encrypts data in transit using the TLS protocol. However, Sally identifies several servers that are still using the

[21] De-identified data can be combined with other datasets to expose information that was not intended to be deduced from the de-identified dataset. This is called the "mosaic effect."
[22] For more HHS OCR breach statistics, visit https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

vulnerable Secure Sockets Layer version 2 (SSLv2) and version 3 (SSLv3) protocol (see risk 11 in Appendix A). SSLv2 and SSLv3 have known vulnerabilities that allow hackers to defeat the encryption and view the data in transit. Sally works with her IT staff to configure the servers to no longer use SSLv2 and SSLv3.

4.3.1. Encryption to Protect User Devices

Data breaches caused by lost or stolen laptops, phones, external media, and other user devices are still quite common. Breaches involving data that has been rendered unusable, unreadable, or indecipherable to unauthorized persons may not be subject to reporting under breach notification rules. However, encryption is not a "silver bullet," and not all encryption is created equal. There are several questions Sally must consider when deploying encryption into Acme's environment.

Is sensitive data stored on user devices? Even if sensitive data is not intended to be stored, are there other ways for sensitive data to be stored on user devices?

Sensitive data stored on user devices such as laptops, tablets, smartphones, or removable devices such as thumb drives should be encrypted to protect the data. Data that is not stored on user devices, such as data accessed through a web portal, is often protected by other controls, such as application timeouts, encryption of the data in transit, and strong identity management controls. Even if sensitive data is not intentionally stored on user devices, users of applications such as EHRs or RIS may inadvertently or otherwise against company policy store sensitive data on devices in other ways. Mail applications, web browsers, and office productivity software (e.g., spreadsheets or word processing applications) may store data locally on a user device. Even though Acme has a policy that no individually identifiable information should be stored on researcher devices such as laptops, Sally still decides to implement device encryption because of these other ways that data may accidentally or otherwise be stored locally.

At what level will encryption be applied?

Encryption addresses different risks depending on the level at which data is encrypted and how that encryption is implemented. For example, data can be encrypted using:

- Disk-level encryption using self-encrypting disks
- Operating System (OS)-level encryption using features in the operating system
- File-level or folder-level encryption using word processing or Portable Document Format (PDF) application features
- Logical drive-level encryption using encryption software
- Database-level encryption using database features
- Field-level encryption using custom encryption code in the research application and/or database stored procedures

Some of these types of encryption are "transparent" to the user. That is, the system transparently decrypts data for any user that has access to the system. Examples include disk-, OS-, logical drive-, and database-level encryption. Other types of encryption, such as file-level and field-level encryption, separate the encryption key from the user credentials. That is, the user must supply a separate password or encryption key to unlock the data.

Transparent encryption protects against physical loss and theft of data only. For example, transparent database encryption is a good control to mitigate risks due to a hard disk being lost when being transferred from a data center to a backup location. However, transparent database encryption does not help if a hacker compromises the account of a database administrator. Because the administrator has access to the system, the database software transparently decrypts the data for the user, fraudulent or not. Field-level encryption, on the other hand, may help address this risk. The database administrator needs system access to perform database maintenance, but does not have business need to access the data itself. In this case, the database administrator could be provisioned with system access but not given access to the decryption key. In this manner, a hacker would have to compromise both the key and the user account before accessing the data. In security theory, this is called "separation of duties."

How will encryption keys be stored?

Sally must also determine how encryption keys will be stored. Encryption keys should not be stored alongside the data they are protecting. For instance, in the field-level encryption example discussed above, if the field-level encryption key were stored in the database, the database administrator (or a criminal purporting to be the administrator) would have access to the key rendering the field-level encryption meaningless. Encryption keys themselves should be stored encrypted. Data-encrypting keys (keys used to encrypt data) and key-encrypting keys (keys used to encrypt keys) should be stored separately.

What happens if an encryption key is lost or compromised?

Sally also makes plans in case an encryption key is lost or compromised. Data cannot be decrypted without an encryption key. Therefore, if the only copy of a key is lost (e.g., deleted), then that data becomes inaccessible. Just as organizations maintain data backups, an encryption key backup program should be established to avoid the unavailability of data due to inability to decrypt.

On the other hand, if an encryption key is compromised by a hacker, the encrypted data could be compromised as well. Sally updates Acme's encryption policies to address this risk by outlining key rotation procedures. These procedures may include setting new encryption keys, decrypting existing data using the old keys, and re-encrypting it using the new keys.

4.3.2. Securing of User Credentials

User credentials such as passwords also should be protected, as encryption controls can be subverted if a hacker compromises a legitimate user's account. Instead of creating separate user credentials for each application, organizations should rely on well utilized credential systems such as Active Directory or OAuth-based credentials where possible. These systems have been scrutinized and well tested to ensure they do not have security vulnerabilities.

When custom user credentials need to be used, passwords should never be stored in plaintext but rather stored using a one-way hash[23] such as Secure Hash Algorithm 2 (SHA-2). However, simply hashing a password is not enough. The latest NIST guidance[24] describes how passwords should be stored.

[23] Passwords should not be stored encrypted. Encrypted passwords can be retrieved if a hacker gains access to the encryption key, introducing an additional risk. Rather, passwords should be stored using one-way hashes to prevent this risk.
[24] Password storage information is available in the NIST Special Publication 800-63B at https://pages.nist.gov/800-63-3/sp800-63b.html.

4.4. Vendor Management

Acme depends on services and software provided by vendors and subcontractors to perform PMI research. Some vendors represent little risk to Acme's data and systems. For example, a landscape contractor that provides grounds maintenance and has no facility access is a very low risk. Other vendors that work with PMI data are at a higher risk, such as subcontractors that provide IT support or researchers from other institutions performing research on Acme's behalf.

As a first step to reducing risks from vendor vulnerabilities, Sally catalogs existing vendors and their level of access to PMI data. This step is challenging because no business unit within Acme maintains a list of vendors. Sally works with the accounts payable department to identify vendors that are receiving payment from Acme, then works with the internal team who charged the payment to identify what services the vendor provides to Acme. Once she has identified Acme's vendors, she separates the vendors into categories based on their level of access to PMI data.

During the security risk assessment, Sally identifies several security risks that could be caused by vendors with the highest level of access to PMI data, including security risks related to Open Source Software (OSS), Commercial Off-the-Shelf (COTS) software, remote support services, and legacy products (see Risks 14, 16, and 17 in Appendix A). For these vendors, Sally works with Acme's legal team to review their contracts and ensure that they contain appropriate provisions for the protection of PMI data that the vendor may use or maintain. These provisions also include the requirement that vendors provide satisfactory assurances that their security controls are working as intended, such as evidence that they provide privacy and security training to their staff, have an independent security firm review their security controls, and have appropriate authentication, authorization, and identity proofing processes in place.

4.4.1. Open Source Software (OSS)

OSS is software that has its source code available under license. The open source license may place additional restrictions on the reuse of the source code, such as requiring any modifications to the source code to also be released under an open source license. Many OSS projects allow developers to contribute code, bug fixes, and features to the project. Some OSS projects have robust support communities and are used in mission-critical applications such as the Linux operating system and the Apache Tomcat web server. These projects typically have a strong change control structure that requires review and approval by senior developers/administrators prior to a new developer contributing code. Other OSS projects are "dead" with no support community or change control structure.

The use of OSS is widespread and integral to modern software development. OSS speeds up software development and allows for higher quality software by leveraging existing, well-known libraries, particularly for specialized functionality. For example, the ability to print a document to PDF is a common feature supported by many types of software. It is faster and cheaper for a developer to leverage a well-known, high-quality OSS library instead of developing PDF printing code for each project.

OSS is not inherently less secure than commercial software. Use of OSS, however, can introduce several risks to Acme's PMI data:

- PMI Data Confidentiality – Security vulnerabilities in OSS or poorly configured software can expose PMI data to unauthorized disclosure.
- PMI Data Integrity – Functional defects in OSS can corrupt PMI data; security vulnerabilities in OSS can expose PMI data to unauthorized modification.

- PMI Data Availability – OSS cannot provide support if software causes mission-critical system failures.

Another risk unique to OSS is that an organization may not be aware of what OSS it is using. Because OSS source code is freely available for download, software developers may include OSS libraries or portions of OSS libraries. Often, OSS licenses require attribution that the software is being used in a commercial product, but it is incumbent on software developers to follow the terms of these licenses.

To mitigate risks from OSS, Sally first works with her IT staff to identify existing OSS deployed by Acme. This includes obtaining bills of material from commercial software vendors to identify OSS that may be used within their products as well. Sally then reviews the OSS community support for each of those projects, such as the last time the project was updated or if there is a dedicated developer forum or community for the project. For "dead" projects that have little or no active support, Sally works with her IT staff to develop a multi-year plan to phase out this legacy software. For well-supported projects, Acme's IT staff reviews the deployment configuration to ensure it is deployed securely.

During her review of Acme's OSS, Sally identifies that Acme is using several OSS libraries that are out of date. She works with her IT staff to update these libraries to ensure they have the latest security patches installed. Sally also includes Acme's OSS applications and libraries in its system management program to monitor for new vulnerabilities and bugs to ensure patches are identified and applied as soon as possible.

4.4.2. Commercial Off-the-Shelf (COTS) Software

COTS software is vendor-provided software that is not custom-built for the organization. Examples are operating systems or word processing software. Like OSS, COTS software can introduce security risks to the confidentiality, integrity, and availability of PMI data. To address risks from COTS, Sally adopts a plan similar to the one for addressing risks from OSS. First, she works with the IT department to identify COTS vendors, then reviews the existing contracts and licensing agreements for these vendors.[25] She ensures that Acme has contractual guarantees on how long a vendor has to release a patch once a vulnerability is identified in the product while ensuring that all patches are up-to-date. Additionally, Sally ensures that software escrow agreements are in place; escrow agreements help ensure that Acme retains access to software even if the vendor goes out of business.

Sally also ensures that Acme has some assurances in the security of the software products it purchases from vendors. Most often, vendors will provide evidence that they have performed application security testing on their products using an independent third-party firm;[26] this evidence may be in the form of an executive summary letter from the security firm. Third-party application security testing is particularly helpful for gaining confidence that cloud service providers are secure, as Acme does not have a copy of their software to test themselves. For products that are deployed within Acme's environment, Sally includes them in the organization's own security testing plans to test their security configuration.

4.4.3. Remote Support Services

Several vendors provide remote support services — vendor support personnel have the ability to remotely access Acme systems to provide support. Oftentimes, vendor support personnel need system

[25] For more information on EHR contracts, access https://www.healthit.gov/sites/default/files/EHR_Contracts_Untangled.pdf.
[26] This type of testing is also known as ethical hacking or penetration testing.

administrator access to provide support. Currently, support personnel use a shared account for accessing Acme's systems. This introduces several security risks to Acme's environment.

First, any changes that support personnel make cannot be tracked at the individual level. Acme knows that *someone* on vendor support staff made a change, but not *who* on the support staff made the change. Second, former contractors and vendor employees may know the shared system account and be able to access Acme's systems and servers.

Sally works with Acme's vendors to remove shared user accounts. For example, Sally sets up a procedure so that when a vendor support user needs to access Acme systems remotely, they first call an Acme IT user who creates an individual user account for the vendor support user.

4.4.4. Securing of Legacy Products

As a best practice, organizations should ensure that systems are kept up-to-date with the latest security patches. However, legacy products may not have security patches available, or they may require legacy operating systems that are no longer supported by their developers.

Sally identifies a legacy RIS during her security risk assessment (see Section 3.3). To address risks in this legacy system, Sally works with her IT team to move the legacy systems to a separate network segment. The firewall for this network segment blocks outgoing and incoming traffic, except from a dedicated "jump" box. To access the legacy RIS, a researcher first must authenticate to the jump box using two-factor authentication, then the researcher can remote-desktop into the legacy RIS from the jump box.

4.5. Physical Security

In addition to the technical security controls that she has reviewed so far, Sally must also consider the physical security of Acme's computing resources and PMI data (see Risk 13 in Appendix A). At Acme, a separate facilities manager within the HR department handles personnel security. She is responsible for ensuring that Acme's workplaces are safe and secure by ensuring, for example, that fire systems are up to code, that employees receive training to prepare for an "active shooter" scenario, and that workspaces are up-to-date with the latest federal and state workplace safety laws. As such, Sally focuses her attention on risks to the physical security of PMI data.

Most of Acme's PMI data is stored inside a secure data center. The data center service provider has a third-party auditor perform annual reviews of the service provider's physical security. However, Acme does not have access to those reviews. Sally works with her service provider to obtain an executive summary letter of the review signed by the third-party auditor. The letter attests to the quality of the security controls in place.

In addition to PMI data stored at the data center, Acme users may inadvertently or otherwise store PMI data on laptops and other mobile devices. As discussed previously, Sally implements an encryption program to ensure that any PMI data stored on these devices is secure in the event that a device is lost or stolen (see Section 4.3).

4.6. Security Policy & Procedure

During her security risk assessment, Sally reviews Acme's policies and procedures to make sure they are up-to-date and responsive to security threats and user needs. In particular, she focuses on education and awareness to ensure that each Acme user is aware of his/her responsibilities to safeguard PMI data (see Risk 10 in Appendix A).

Acme users feel that the current privacy and security awareness training they receive is not relevant to their daily tasks. Sally sits down with users from different business units to understand what they do on a daily basis. She then adapts the privacy and security awareness training to be more applicable to these users. For example, users cited the frequent need for transferring large files — files that are too large to be emailed. However, not all business units had access to a file transfer server, and the security awareness training did not address how to transfer large files securely. Several users were tempted to use their own private cloud accounts for transferring files, which is against company policy. To address this risk, Sally works with her IT team to make file transfer servers available to all users for internal file transfers, and she adds a topic on "how to transfer large files" to the awareness training.

4.7. PMI Organizations & the HIPAA Rules

Throughout this guide, the use case has assumed that Acme is not subject to the HIPAA Rules. However, organizations using PMI data for research purposes may be a covered entity or business associate subject to the HIPAA Rules. Further, contractors supporting a HIPAA covered entity's or business associate's use of PMI data may also be subject to the HIPAA Rules as a business associate. If an organization is unsure whether or not it is subject to the HIPAA Rules as a HIPAA covered entity or business associate, it is encouraged to review OCR's guidance on this matter.[27]

Organizations that work with PMI data and are subject to the HIPAA Rules are required to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of Protected Health Information (PHI) in accordance with the requirements of the HIPAA Rules; this includes PMI data that also meets the definition of PHI.[28] Information on the HIPAA Rules, including guidance and resources for compliance, is available on OCR's website.[29]

This guide provided an example of conducting a security risk assessment and applying controls to protect the PMI data held by Acme. Although conducting an enterprise-wide risk assessment is beyond the scope of this document, an enterprise-wide risk assessment is required by the HIPAA Security Rule. More specifically, a HIPAA covered entity or business associate must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of the ePHI that the covered entity or business associate creates, receives, maintains, or transmits throughout its entire enterprise.

After conducting its risk assessment, the covered entity or business associate must implement security measures sufficient to reduce the identified risks and vulnerabilities to a reasonable and appropriate level. OCR's guidance on conducting a risk assessment, as well as additional HIPAA Security Rule guidance and compliance resources, is available on OCR's website.[30]

When PMI organizations that are subject to the HIPAA Rules conduct and update security risk assessments and implement security measures, this can help them implement the PMI Data Security

[27] OCR guidance on covered entities and business associates is available at http://www.hhs.gov/hipaa/for-professionals/covered-entities/.
[28] The definition of PHI is available at http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/#protected.
[29] For OCR guidance and resources on complying with the HIPAA Rules, visit http://www.hhs.gov/hipaa/for-professionals/index.html.
[30] For guidance on the Security Rule and conducting a risk assessment, visit OCR's website at http://www.hhs.gov/hipaa/for-professionals/security/index.html.

Principles. Furthermore, Appendix B provides a crosswalk that maps HIPAA Security Rule standards and implementation specifications to PMI Data Security Principles. This crosswalk can help entities covered by HIPAA leverage their existing HIPAA compliance activities when implementing the PMI Data Security Policy Principles.

5. Other Actions Taken to Secure PMI Data & Systems & Move Forward

In addition to the key themes listed in Section 4, during her security risk assessment Sally identifies several gaps to be addressed, such as creating a public website with ways to contact the Acme security team, or updating user training to address common workflows. The full list of gaps she identifies is listed in Appendix A.

Recognizing that not all security risks can be addressed immediately due to time and resource constraints, Sally prioritizes the gaps based on risks to the organization and time/resources it will take to address the risk. Finally, she develops a three-year project plan to address the gaps and presents it to her executive leadership and board of directors.

Security risks are not static. To keep her security risk assessment up-to-date, Sally meets with business units on a quarterly basis to determine what environmental and operational changes have been made, then updates her risk assessment accordingly. Sally keeps up-to-date with security news sites, mailing lists, and information sharing organizations. On a yearly basis, she reviews the entire security risk assessment for changes to ensure that Acme stays protected from security risks.

Appendix A: Example Cybersecurity PMI Target Profile

Risk #	Cyber-security Framework (CSF) Category[31]	PMI Data Security Principle	Threats	Mitigating Controls	Gaps	CVSSv3 Base Score Metrics	CVSSv3 Temp-oral Score Metrics	CVSSv3 Env Score Metrics	CVSSv3 Overall Score
1	ID.BE ID.GV	Overall Security Plan	Outlined below	Outlined below	Outlined below	N/A	N/A	N/A	N/A
2	ID.BE ID.GV ID.RA ID.RM	Risk-Based Approach	None known	This security risk assessment, to be repeated annually or upon a major environment change	None known	N/A	N/A	N/A	N/A
3	ID.RA	Independent Third-Party Review	1. Hacker takes advantage of unpatched vulnerabilities	1. Acme conducts vulnerability scans quarterly	1. No penetration testing is being performed on network	8.1	8.1	8.1	8.1
	ID.RA	Independent Third-Party Review	2. Hacker tricks users into downloading malicious files/ disclosing passwords	2. Acme provides user awareness and training	2. Based on user interviews, security awareness training does not address common user workflows	6.8	6.3	6.2	6.4
4	Principle does not align with a CSF category	Transpar-ency	1. User has no means to submit user-identified security vulnerabilities	1. None	1. There is no publicly available website with security contact information	5.5	5.2	3.8	4.8

[31] For more information on NIST Cybersecurity Framework categories, visit https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

Risk #	Cyber-security Framework (CSF) Category[31]	PMI Data Security Principle	Threats	Mitigating Controls	Gaps	CVSSv3 Base Score Metrics	CVSSv3 Temp-oral Score Metrics	CVSSv3 Env Score Metrics	CVSSv3 Overall Score
5	PR.AC	Identity Proofing	1. Hacker impersonates user and convinces IT admin to create new user credentials for hacker	1. Acme covers this as part of the onboarding/HR process; it is out of scope for this risk assessment	1. Sally notes this risk for future risk assessments of the onboarding/HR process	N/A	N/A	N/A	N/A
	PR.AC	Identity Proofing	2. Hacker impersonates a user and convinces IT admin to reset a user's credential through the Help Desk	2. Users are required to take annual Privacy and Security (P&S) awareness and training	2. Based on user interviews, security awareness training does not address common user workflows	6.8	6.3	6.2	6.4
	PR.AC	Identity Proofing	3. Hacker spoofs knowledge-based questions to reset a user's credential through a self-help portal	3. Knowledge-based questions are provided	3. Knowledge-based questions are easily spoofed	7.1	6.9	7.3	7.1
6	PR.AC	Credentials	1. Hacker guesses weak user password	1. Systems require complex passwords	1. Complex passwords are not strong in practice	7.3	6.9	7.6	7.3

Risk #	Cyber-security Framework (CSF) Category[31]	PMI Data Security Principle	Threats	Mitigating Controls	Gaps	CVSSv3 Base Score Metrics	CVSSv3 Temp-oral Score Metrics	CVSSv3 Env Score Metrics	CVSSv3 Overall Score
	PR.AC	Credentials	2. User selects easily guessed password	2. None known	2. Complex passwords are difficult to remember	7.3	7.1	7.8	7.4
7	PR.AC	Auth-entication	1. Hacker gains fraudulent user access	1. All users must authenticate to both the Virtual Private Network (VPN) and analysis software	1. User authentication relies on a single factor	5.0	4.7	4.4	4.7
	PR.AC	Auth-entication	2. Hacker gains fraudulent admin access	2. All admins must authenticate at both the network and server level	2. Admin authentication relies on a single factor	5.0	4.7	5.2	5.0
	PR.AC	Auth-entication	3. Hacker bypasses application user interface and accesses web server directly	3. APIs use application token for authentication	3. Application token is hard-coded in software	5.3	5.3	7.1	5.9
8	PR.AC	Authoriza-tion	1. User accesses data not appropriate for his/her role	1. Consent management system access rules determine what information a user can view	1. None known	N/A	N/A	N/A	N/A

Risk #	Cyber-security Framework (CSF) Category[31]	PMI Data Security Principle	Threats	Mitigating Controls	Gaps	CVSSv3 Base Score Metrics	CVSSv3 Temp-oral Score Metrics	CVSSv3 Env Score Metrics	CVSSv3 Overall Score
9	PR.AT	Participant Education	1. Participants lose confidence in P&S and withdraw from studies	1. None known	1. There is no publicly available website with security contact information	5.5	5.2	3.8	4.8
10	PR.AT	PMI Data User Education	1. Sloppy user behavior leads to inadvertent disclosure of research data	1. Users are required to take annual P&S awareness and training	1. Based on user interviews, security awareness training does not address common user workflows	6.8	6.3	6.2	6.4
11	ID.AM PR.DS	Encryption	1. Research data is compromised on lost/stolen laptop/device	1. Users are only supposed to have aggregate results on laptop/devices	1. Users may ignore policy and store identifiable data on laptop/devices	6.1	6.1	6.8	6.3
	ID.AM PR.DS	Encryption	2. Hacker exfiltrates data from the database after gaining fraudulent access	2. Direct identifiers are stored separately from research data	2. Compromise of direct Identifiers DB may still be a data breach under state law	8.1	8.1	8.6	8.3
	ID.AM PR.DS	Encryption	3. Information is disclosed when transmitted over the Internet	3. Data flows are protected by VPN and SSH	3. None known	N/A	N/A	N/A	N/A

Risk #	Cyber-security Framework (CSF) Category[31]	PMI Data Security Principle	Threats	Mitigating Controls	Gaps	CVSSv3 Base Score Metrics	CVSSv3 Temp-oral Score Metrics	CVSSv3 Env Score Metrics	CVSSv3 Overall Score
	ID.AM PR.DS	Encryption	4. Hacker takes advantage of obsolete encryption solution	4. Encryption solutions are patched and up-to-date	4. Several Acme servers use SSLv2 and SSLv3, both of which have known vulnerabilities	7.4	6.4	6.4	6.7
12	PR.DS	Encryption Key Security	1. Hacker gains access to encryption key used to protect information in transit	1. Encryption keys are stored in OS certificate store	1. None known	N/A	N/A	N/A	N/A
13	ID.AM PR.AC	Physical Security	1. Hacker gains physical access to laptop/device	1. Users are only supposed to have aggregate results on laptop/devices	1. Users may ignore policy and store identifiable data on laptop/devices	6.1	6.1	6.8	6.3
	ID.AM PR.AC	Physical Security	2. Hacker gains physical access to servers	2. Data center security is managed by service provider	2. Service provider provides no proof that security controls are in place/effective	6.7	6.3	7.2	6.7
	ID.AM PR.AC	Physical Security	3. Employee loses laptop/device while working remote	3. Users are only supposed to have aggregate results on laptop/devices	3. Users may ignore policy and store identifiable data on laptop/devices	6.1	6.1	6.8	6.3
14	ID.GV	Service Provider Security	1. Weak data center security allows hackers physical access to servers	1. Data center security is managed by service provider	1. Service provider provides no proof that security controls are in place/effective	7.3	7.3	7.3	7.3

Risk #	Cyber-security Framework (CSF) Category[31]	PMI Data Security Principle	Threats	Mitigating Controls	Gaps	CVSSv3 Base Score Metrics	CVSSv3 Temp-oral Score Metrics	CVSSv3 Env Score Metrics	CVSSv3 Overall Score
	ID.GV	Service Provider Security	2. Analysis software vendor has remote access for support; hacker compromises remote access connection	2. Analysis software vendor support users log in to remote access solution as well as OS	2. Analysis software vendor support users share OS user accounts	8.3	8.3	8.4	8.3
	ID.GV	Service Provider Security	3. Hacker takes advantage of unpatched system	3. Security patches from vendors are applied on a regular basis	3. OSS deployed on web server does not have an automatic update feature	8.4	8.4	8.4	8.4
15	PR.DS	Integrity Protection	1. Hacker makes fraudulent data edit	1. Edits are tracked in the audit log	1. None known	N/A	N/A	N/A	N/A
	PR.DS	Integrity Protection	2. Hacker makes fraudulent audit log edit	2. None known	2. Admin users have access to make edits to both data and the audit log	4.2	4.2	6.0	4.8
16	ID.BE PR.IP	Information System Life Cycle	1. Hacker takes advantage of vulnerabilities in IT products	1. Purchasing staff ask vendors to answer standard security questionnaire	1. Acme is relying on vendor attestation that security has been built into product	9.6	8.1	8.0	8.6

Risk #	Cyber-security Framework (CSF) Category[31]	PMI Data Security Principle	Threats	Mitigating Controls	Gaps	CVSSv3 Base Score Metrics	CVSSv3 Temp-oral Score Metrics	CVSSv3 Env Score Metrics	CVSSv3 Overall Score
17	PR.MA	Security Patching	1. Hacker takes advantage of unpatched system	1. Patches are applied monthly, with emergency patches reviewed for impact to operations and security risk	1. None known	N/A	N/A	N/A	N/A
	PR.MA	Security Patching	2. Unpatched OSS vulnerabilities can be exploited to allow unauthorized access	2. Acme identifies and incorporates all instances of open source and third-party software in use in organization's patch management plan	2. Open source and third-party vendors patch infrequently with little or no announcement of new vulnerabilities or available patches	9.6	8.1	8.0	8.6
18	PR.PT	Audit Events	1. Rogue user performs unauthorized action	1. Audit trail captures create, read, update, delete, copy, print, query, and user privilege change actions	1. None known	N/A	N/A	N/A	N/A
	PR.PT	Audit Events	2. Hacker remains undetected on network after gaining fraudulent access to user account	2. Alerts are generated when actions fall outside norms (e.g., logins at 3 a.m.)	2. None known	N/A	N/A	N/A	N/A

Risk #	Cyber-security Framework (CSF) Category[31]	PMI Data Security Principle	Threats	Mitigating Controls	Gaps	CVSSv3 Base Score Metrics	CVSSv3 Temp-oral Score Metrics	CVSSv3 Env Score Metrics	CVSSv3 Overall Score
19	PR.PT	Audit Logs	1. Hacker tampers with audit log to hide nefarious behavior	1. None known	1. Audit log lacks tampering detection	4.2	4.2	6.0	4.8
	PR.PT	Audit Logs	2. Audit log system goes down, allowing hacker to hide nefarious behavior	2. None known	2. Audit log messages lack guaranteed delivery	4.2	4.2	6.0	4.8
20	DE.AE DE.CM DE.DP	Detection and Alerting	1. Users inadvertently facilitate propagations of malicious software	1. Antivirus software alerts IT staff of propagation attempts	1. Antivirus solution may not recognize newest variants of malicious software	9.1	8.0	8.7	8.6
	DE.AE DE.CM DE.DP	Detection and Alerting	2. Under-reporting leads to nefarious activity being overlooked	2. Acme conducts risk-based assessment of system activities that should be audited	2. None known	N/A	N/A	N/A	N/A

Risk #	Cyber-security Framework (CSF) Category[31]	PMI Data Security Principle	Threats	Mitigating Controls	Gaps	CVSSv3 Base Score Metrics	CVSSv3 Temp-oral Score Metrics	CVSSv3 Env Score Metrics	CVSSv3 Overall Score
	DE.AE DE.CM DE.DP	Detection and Alerting	3. "Alert fatigue" leads to nefarious activity being overlooked	3. Acme conducts: user awareness and training; generous time-off policy to avoid employee burn out; periodic audits of random 5% of logs for missed activity	3. None known	N/A	N/A	N/A	N/A
21	ID.RA RS.CO	Threat Information Sharing	1. Hacker uses techniques perfected against other PMI organizations to hack Acme	1. Acme participates in relevant threat sharing organizations	1. Acme does not participate in threat sharing organizations	6.3	5.9	5.9	6.0
22	ID.RM PR.IP RS.CO	Anomaly Reporting	1. Lack of executive support and oversight leads to less security program participation	1. Quarterly reports of security incidents and security program progress are presented to compliance board quarterly	1. None known	N/A	N/A	N/A	N/A

Risk #	Cyber-security Framework (CSF) Category[31]	PMI Data Security Principle	Threats	Mitigating Controls	Gaps	CVSSv3 Base Score Metrics	CVSSv3 Temp-oral Score Metrics	CVSSv3 Env Score Metrics	CVSSv3 Overall Score
23	PR.IP RS.RP RS.AN	Incident Response	1. Security intrusions are not properly handled, allowing hackers to remain on network	1. Incident response plan is developed and documented	1. Response plan depends on key personnel with little redundancy	6.5	6.5	8.3	7.1
	PR.IP RS.RP RS.AN	Incident Response	2. Security intrusions are not properly investigated, leaving breaches undiscovered	2. Incident response plan is developed and documented	2. There is no computer forensic team on retainer	6.3	6.3	6.3	6.3
24	PR.IP	Incident Response Testing	1. Failure to regularly test incident response plans can lead to confusion and mismanage-ment during response plan execution	1. Incident response plan is tested every two years	1. Incident response plan testing is not happening quarterly	5.3	5.3	6.1	5.6
25	RS.CO	Affected Individual Notification	1. Organization fails to notify individuals affected by a breach	1. Breach notification plan is developed and documented	1. None known	N/A	N/A	N/A	N/A

Risk #	Cyber-security Framework (CSF) Category[31]	PMI Data Security Principle	Threats	Mitigating Controls	Gaps	CVSSv3 Base Score Metrics	CVSSv3 Temp-oral Score Metrics	CVSSv3 Env Score Metrics	CVSSv3 Overall Score
26	ID.GV	Accountable Point of Contact	1. Lack of a single accountable point of contact can lead to a disjointed response	1. Point of contact is documented in incident response plan	1. Response plan depends on key personnel with little redundancy	6.5	6.5	8.3	7.1
27	RS.MI RC.RP	Incident and Breach Recovery Plan	1. Lack of a recovery plan can lead to system unavailability following a security incident	1. Incident recovery plan is tested every two years	1. Incident recovery plan testing is not happening quarterly	5.3	5.3	6.1	5.6
28	RS.CO RC.CO	Communica-tion	1. Lack of clear communica-tion can lead to reputational harm as stakeholders assume the worst	1. Communication plan and templates are included in breach response plan	1. None known	N/A	N/A	N/A	N/A
29	RS.IM RC.IM	Lessons Learned	1. Mistakes can be repeated if root causes of security incidents are not addressed	1. Incident recovery plan requires root cause analysis as part of post-incident close out	1. None known	N/A	N/A	N/A	N/A

Appendix B: Crosswalk between HIPAA Security Rule and PMI Data Security Principles

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
IDENTIFY	**Overall Security Plan:** PMI organizations should develop a comprehensive risk-based security plan that outlines roles and responsibilities related to security, consistent with the principles and framework outlined here. The security plan should identify the governance body for the organization's security program. The governance body will ensure those who use or manage PMI data adhere to the security plan. The security plan should be reviewed by the governance body and updated periodically to incorporate evolving standards and best practices. The plan should describe its approach for: complying with applicable laws and regulations and other organization-specific security policies and standards; designating and maintaining an appropriately resourced and technically experienced information security team; identifying, assessing, and responding to vulnerabilities and threats; conducting continuous monitoring; responding to security incidents and breaches; ensuring the physical security of areas where PMI data is located; and ensuring participants, researchers, and technical staff are aware of their security responsibilities.	**§ 164.308(a)(1)(i): Security management process:** Implement policies and procedures to prevent, detect, contain, and correct security violations. **§ 164.308(a)(2): Assigned security responsibility:** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate. **§ 164.308(a)(3)(i): Workforce security:** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information. **§ 164.314(b): Updates:** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
IDENTIFY	**Risk-Based Approach:** PMI organizations should use risk-management strategies, tools, and techniques to inform and prioritize decisions regarding the protection of PMI data, including electronic and physical resources within its environment as well as at the point of initial collection. When planning protection of PMI data, the form of the data should be considered (e.g., raw, aggregate, the product of a mathematical or statistical process or an analysis report, as well as whether the data are electronic or paper-based).	**§ 164.308(a)(1)(ii)(A): Risk analysis:** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity or business associate. **§ 164.308(a)(1)(ii)(B): Risk management:** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Although the HIPAA Security Rule addresses the safeguards that must be applied to protect PHI in electronic form, the HIPAA Privacy Rule requires that appropriate administrative, physical, and technical safeguards are in place to protect the privacy of PHI in any form, including paper-based (§ 164.530(c)(1)).

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
IDENTIFY	**Independent Third-Party Review:** PMI organizations should have an independent review of their security plans and of the effectiveness of controls on a periodic basis. The reviewer, at a minimum, should perform: a review of the organization's adherence to its security plan; regular vulnerability assessments (e.g., network scans and penetration testing); and evaluation and adjustment of the security program in light of vulnerability assessments and evolving circumstances.	There is not a specific Security Rule requirement regarding an independent third-party review of an organization's security posture or HIPAA compliance. However, conducting network scans and penetration tests should be included as part of an entity's security program and would be a very important part in conducting an accurate and thorough assessment of the potential risks and vulnerabilities to ePHI as called for in the HIPAA Security Rule's Risk Analysis requirement. **§ 164.308(a)(8): Evaluation:** Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	None
IDENTIFY	**Transparency:** A high-level overview of the organization's security plan and approach should be posted publicly to help enable transparency and congruity with the goals of the Privacy and Trust Principles and this Security Framework. This high-level overview should describe the organization's breach notification process, steps individuals should take to protect themselves, and ways that the public and users of the PMI data can easily submit information about potential vulnerabilities and bugs.	There is not a specific Security Rule requirement regarding the public posting of an organization's security plan. However, applicable covered entities must include a statement in the Notice of Privacy Practices provided to individuals indicating that they will be notified if there is a breach of their unsecured PHI (§ 164.520(b)(1)(v)(A)).	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
PROTECT	**Identity Proofing:** PMI organizations should develop a policy for verifying the identity of users and contributors (e.g., participants and health care provider organizations), prior to granting credentials for access to or contribution of PMI data.	**§ 164.312(d): Person or entity authentication:** Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	The level of identity proofing required should be determined as a result of the PMI organization's risk analysis.
PROTECT	**Credentials:** PMI organizations should use innovative approaches for authentication so that over time they do not rely on username and password alone. They should use strong multi-factor authentication for users of PMI data.	**§ 164.312(a)(2)(i): Unique user identification:** Assign a unique name and/or number for identifying and tracking user identity. **§ 164.312(d): Person or entity authentication:** Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	None
PROTECT	**Authentication:** Risk-based authentication controls should flow from the PMI organization's security risk assessment and should be commensurate with the type of data, level of sensitivity of the information, and user type.	**§ 164.312(a)(1): Access control:** Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
PROTECT	**Authorization:** Authorization controls should be granular enough to support participant consent that has been captured by the PMI organization and should limit access, use, or disclosure based on what is necessary to satisfy a particular purpose or carry out a function.	**§ 164.308(a)(4)(i): Information access management:** Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of subpart E of this part. **§ 164.308(a)(4)(ii)(B): Access authorization:** Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism. **§ 164.308(a)(4)(ii)(C): Access establishment and modification:** Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	None
PROTECT	**Participant Education:** PMI organizations should provide participants with security awareness materials and education on an ongoing basis. The educational materials should include discussion of how data will be used, the high-level protections that safeguard the data, and the tools available to research participants to protect their own PMI data.	The Security Rule Security Awareness and Training requirements are applicable to an entity's workforce (staff and management) and not directly applicable to participants.	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
PROTECT	**PMI Data User Education:** PMI organizations should provide appropriate training for individuals using PMI data and infrastructure based on the individual's role and responsibilities. This role-based training should include information on appropriate protections for PMI data and security best practices. Appropriate security certifications and continued training in information system security and privacy protection should be encouraged.	**§ 164.308(a)(5)(i): Security awareness and training:** Implement a security awareness and training program for all members of its workforce (including management). **§ 164.308(a)(5)(ii)(A): Security reminders:** Periodic security updates. **§ 164.308(a)(5)(ii)(B): Protection from malicious software:** Procedures for guarding against, detecting, and reporting malicious software. **§ 164.308(a)(5)(ii)(C): Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies. **§ 164.308(a)(5)(ii)(D): Password management:** Procedures for creating, changing, and safeguarding passwords.	None
PROTECT	**Encryption:** PMI data that is reasonably likely to identify an individual should be protected at-rest and in-motion using strong encryption. Examples of data reasonably likely to identify an individual include direct identifiers such as name, birth date, contact information, and Social Security Number.	**§ 164.312(a)(2)(iv): Encryption and decryption:** Implement a mechanism to encrypt and decrypt electronic protected health information. **§ 164.312(e)(2)(ii): Encryption:** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
PROTECT	**Encryption Key Security:** PMI organizations should store encryption keys separately from encrypted data and establish policies for secure encryption key creation, distribution, access, and revocation.	Although there is not a specific Security Rule requirement regarding encryption key management, it is expected that covered entities and business associates would establish policies and procedures regarding encryption key management as appropriate in accordance with the implementation of encryption security measures (§ 164.312(a)(2)(iv) and § 164.312(e)(2)(ii)).	OCR's "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals" requires that the confidential process or key used to encrypt data be secure in order for PHI to be considered secure for purposes of HIPAA breach notification requirements. This guidance continues stating that "[t]o avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt."

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
PROTECT	**Physical Security:** PMI data should be protected by physical security controls as well as cybersecurity controls.	**§ 164.310(a)(1): Facility access controls:** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. **§ 164.310(a)(2)(ii): Facility security plan:** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. **§ 164.310(a)(2)(iii): Access control and validation procedures:** Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. **§ 164.310(a)(2)(iv): Maintenance records:** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). **§ 164.310(b): Workstation use:** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI. Continued on next page	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
PROTECT	**Physical Security, continued:** PMI data should be protected by physical security controls as well as cybersecurity controls.	**§ 164.310(c): Workstation security:** Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users. **§ 164.310(d)(1): Device and media controls:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and the movement of these items within the facility. **§ 164.310(d)(2)(i): Disposal:** Implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored. **§ 164.310(d)(2)(ii): Media re-use:** Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. **§ 164.310(d)(2)(iii): Accountability:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
PROTECT	**Service Provider Security:** When PMI organizations employ subcontractors, third parties, or vendors (including hosted, cloud, or application service providers) to create, receive, maintain, or transmit PMI data, PMI organizations should obtain the necessary assurances that the service provider will appropriately safeguard PMI data, consistent with the PMI organization's security plan.	**§ 164.308(b)(1): Business associate contracts and other arrangements:** A covered entity may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. **§ 164.308(b)(2):** A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit ePHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information. **§ 164.308(b)(3): Written contract or other arrangement:** Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	§ 164.314 (Organizational Requirements) includes specific requirements for business associate contracts.
DETECT	**Audit Events:** PMI organizations should define a set of system and network events that capture interactions with PMI data from networks, servers, and application infrastructure, including user access and behavior.	**§ 164.308(b): Audit controls:** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
DETECT	**Audit Logs:** System and network events should be logged on a continuous, uninterrupted basis in a manner that protects against tampering and provides sufficient detail to identify the type of action performed on PMI data, the unique identity of who performed the action, the date and time the action occurred, and the subset of data impacted by the action.	**§ 164.308(b): Audit controls:** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	None
DETECT	**Detection and Alerting:** Continuous detection processes and alerting mechanisms should be created to ensure timely and adequate awareness of anomalous events, as well as a process to inform operational staff and stakeholders with relevant situational details.	**§ 164.308(a)(1)(ii)(D): Information system activity review:** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. **§ 164.308(a)(6)(ii): Response and reporting:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	None
DETECT	**Threat Information Sharing:** PMI organizations should participate in relevant threat information sharing forums. PMI organizations should also follow existing best practices to provide ways for participants and non-affiliated individuals and entities to report potential vulnerabilities or threats and respond to reports appropriately.	Although there is not a specific Security Rule requirement regarding participation in threat information sharing forums or ISAOs, PMI organizations should consider whether participating in cyber-threat information sharing programs is reasonable and appropriate to reduce their security risk.	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
DETECT	**Anomaly Reporting:** PMI organizations should make reports of security anomalies, alerts, reports, or other relevant events available to the PMI organization's governance boards and should also provide remediation plans to prevent similar vulnerabilities from occurring in the future.	**§ 164.308(a)(6)(i): Security incident procedures:** Implement policies and procedures to address security incidents. **§ 164.308(a)(6)(ii): Response and reporting:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	None
RESPOND	**Incident Response:** Not all security incidents result in a breach. PMI organizations should develop a plan to respond to and contain security incidents. This plan should include a process to identify quickly and effectively whether an incident has led to a breach of PMI data. Organizations should coordinate response activities with internal and external parties as appropriate (e.g., law enforcement, Internet Service Providers, ISAOs, Information Sharing and Analysis Centers, and vendors).	**§ 164.308(a)(6)(i): Security incident procedures:** Implement policies and procedures to address security incidents. **§ 164.308(a)(6)(ii): Response and reporting:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
RESPOND	**Incident Response Testing:** PMI organizations should regularly test incident response plans to ensure the highest level of proficiency.	Although there is not a specific Security Rule requirement to regularly test incident response plans, there is a requirement to review and modify security measures to ensure that implemented security measures continue to provide reasonable and appropriate protection of ePHI (§ 164.306(e)). The Security Rule also requires that policies and procedures are reviewed periodically and updated as needed (§ 164.316(b)(2)(iii)).	None
RESPOND	**Affected Individual Notification:** When a PMI organization has determined that a security incident has resulted in a breach of PMI data, the organization should notify the affected individuals and appropriate organizations in accordance with applicable breach notification laws, the Privacy and Trust Principles, and the organization's security plan.	**§ 164.308(a)(6)(ii): Response and reporting:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. If there is a breach of PHI, HIPAA covered entities and business associates are required to provide notice in accordance with the HIPAA Breach Notification Rule (§§ 164.400-414).	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
RESPOND	**Accountable Point of Contact:** PMI organizations should identify an accountable point of contact who will coordinate with appropriate organizations and affected individuals throughout the incident response process. The contact should have the authority to direct actions required in all phases of the incident response.	**§ 164.308(a)(2): Assigned security responsibility:** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	An individual other than the HIPAA privacy or security official may be delegated to act as the Accountable Point of Contact throughout the incident response process; however, the HIPAA security official is ultimately responsible for the development and implementation of security incident response policies and procedures.
RECOVER	**Incident and Breach Recovery Plan:** PMI organizations should establish, maintain, and implement plans for emergency response, backup operations, and post-incident recovery for PMI data. These plans should address how the PMI organization will stabilize after the incident and restore basic services.	**§ 164.308(a)(7)(i): Contingency plan:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. **§ 164.308(a)(7)(ii)(A): Data backup plan:** Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. **§ 164.308(a)(7)(ii)(B): Disaster recovery plan:** Establish (and implement as needed) procedures to restore any loss of data. Continued on next page	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
RECOVER	**Incident and Breach Recovery Plan, continued** PMI organizations should establish, maintain, and implement plans for emergency response, backup operations, and post-incident recovery for PMI data. These plans should address how the PMI organization will stabilize after the incident and restore basic services.	**§ 164.308(a)(7)(ii)(C) Emergency mode operation plan:** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. **§ 164.308(a)(7)(ii)(D): Testing and revision procedures:** Implement procedures for periodic testing and revision of contingency plans. **§ 164.308(a)(7)(ii)(E): Applications and data criticality analysis:** Assess the relative criticality of specific applications and data in support of other contingency plan components. **§ 164.310(a)(2)(i): Contingency operations:** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
RECOVER	**Communication:** As an integral part of the recovery plan, PMI organizations should communicate to stakeholders when a safe and secure environment has been restored.	**§ 164.308(a)(7)(i): Contingency plan:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. **§ 164.310(a)(2)(i): Contingency operations:** Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	None

Cybersecurity Framework Function	PMI Data Security Policy Principle	HIPAA Security Rule Reference	Additional Comments
RECOVER	**Lessons Learned:** After recovery from a security incident or breach, PMI organizations should identify lessons learned, including conducting root cause analysis, to identify areas needing improvement. They should update security plans based on those lessons learned. Lessons learned should be reported to the PMI organization's governance board, and information that may be helpful to other PMI organizations should be shared with the PMI community as appropriate.	**§ 164.308(a)(1)(ii)(A): Risk analysis:** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. **§ 164.308(a)(1)(ii)(B): Risk management:** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with **§ 164.306(a).** **§ 164.308(a)(6)(ii): Response and reporting:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. **§ 164.308(a)(8): Evaluation:** Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	The Security Rule also includes requirements to review and modify implemented security measures to ensure that such measures continue to provide reasonable and appropriate protection of ePHI (§ 164.306(e)) and that implemented policies and procedures are reviewed periodically and updated as needed (§ 164.316(b)(2)(iii)).

Appendix C. HIPAA Safe Harbor De-Identification Method

45 CFR 164.514(b)(2) *Implementation specifications: Requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
(ii) Documents the methods and results of the analysis that justify such determination; or
(2) (2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:
(A) Names;
(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
(D) Telephone numbers;
(E) Fax numbers;
(F) Electronic mail addresses;
(G) Social security numbers;
(H) Medical record numbers;
(I) Health plan beneficiary numbers;
(J) Account numbers;
(K) Certificate/license numbers;
(L) Vehicle identifiers and serial numbers, including license plate numbers;
(M) Device identifiers and serial numbers;
(N) Web Universal Resource Locators (URLs);
(O) Internet Protocol (IP) address numbers;
(P) Biometric identifiers, including finger and voice prints;
(Q) Full face photographic images and any comparable images; and
(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and
(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Appendix D. Additional Resources

- PMI Data Security Policy Principles and Framework
  https://obamawhitehouse.archives.gov/sites/obamawhitehouse.archives.gov/files/documents/PMI_Security_Principles_Framework_v2.pdf

- Security Risk Assessment (SRA) Tool
  https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

- OCR's HIPAA Resources
  http://www.hhs.gov/hipaa/

- NIST Cybersecurity Framework
  https://www.nist.gov/cyberframework

- NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf