JOURNAL OF HEALTH CARE FINANCE

Winter 2020

SECURITY AND PRIVACY OF THE INTEGRATED CLINICAL ENVIRONMENT PART II

JASON LEE WILLIAMS, MSIT, JD, LLM, CIPP/US

INTRODUCTION

Integration without security and privacy is not interoperability. The integrated clinical environment cannot achieve the goals of improving patient safety, increasing treatment effectiveness, and improving operational efficiency without engineering both privacy and security into clinical systems, institutional health information systems, and health information exchanges.

Security and Privacy of the Integrated Clinical Environment is a series of three articles. Part I discussed the basic concepts of interoperability and the integrated clinical environment (ICE), the legal and regulatory framework impacting an interoperable ICE, and an overview of the risks associated with the deployment of an interoperable, ICE. This article, Part II, will discuss the concept of privacy engineering and the various National Institute of Standards and Technology (NIST) frameworks and methodologies, including the new NIST Privacy Framework, that can be utilized to address both privacy and security risk adequately.

PRIVACY ENGINEERING

Privacy engineering is a discipline that systematically addresses privacy risks in a consistent and repeatable manner. When evaluating an interoperable, ICE, privacy must be engineered into the system due to the complex nature of the systems and the sensitivity of the data being processed.

A. *Introduction to Privacy Engineering*

"[P]rivacy engineering means a specialty discipline of systems engineering focused on achieving freedom from conditions that can create problems for individuals with unacceptable consequences that arise from the system as it processes PII."[1] Information security and privacy are not the same, but security is critical to privacy. The disciplines complement one another; therefore, the risk management and systems engineering processes developed for information security can be adapted to address privacy concerns.[2]

Protecting the privacy of an individual's ePHI is not just the job of the privacy or compliance officer, it requires a multidisciplinary approach.[3] The concept of privacy can be challenging to define and often varies depending on the context of the transaction and the value derived from the transaction.[4] However, privacy can be distilled to a straightforward statement, "[P]rivacy exists--or is lost—at the boundary line between the individual and others."[5] Privacy engineering seeks to design effective privacy solutions using a multidisciplinary approach.

---

[1] U.S. DEPT. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH, NISTIR 8062, AN INTRODUCTION TO PRIVACY ENGINEERING AND RISK MANAGEMENT IN FEDERAL SYSTEMS iv (Jan. 2017), https://doi.org/10.6028/NIST.IR.8062 [*hereinafter* NISTIR 8062, AN INTRODUCTION TO PRIVACY ENGINEERING]; *see* MICHELLE DENNEDY ET AL., THE PRIVACY ENGINEER'S MANIFESTO (Kindle Ed. 2014)

[2] NISTIR 8062, AN INTRODUCTION TO PRIVACY ENGINEERING, *supra* note 1.

[3] *Id.* at 6.

[4] *Id.*

[5] *Id.*

Privacy and information security concerns do overlap as an individual cannot have privacy without security.[6] The primary information security objectives are commonly described as CIA, confidentiality, integrity, and availability.[7] Confidentiality plays a vital role in privacy. However, security is only one component of the Fair Information Practice Principles (FIPPs).[8] Security concerns typically arise from an unauthorized activity where privacy concern arises as a byproduct of the authorized processing of personal data.[9] The overlap of privacy and security domains occurs at the issue of data security.

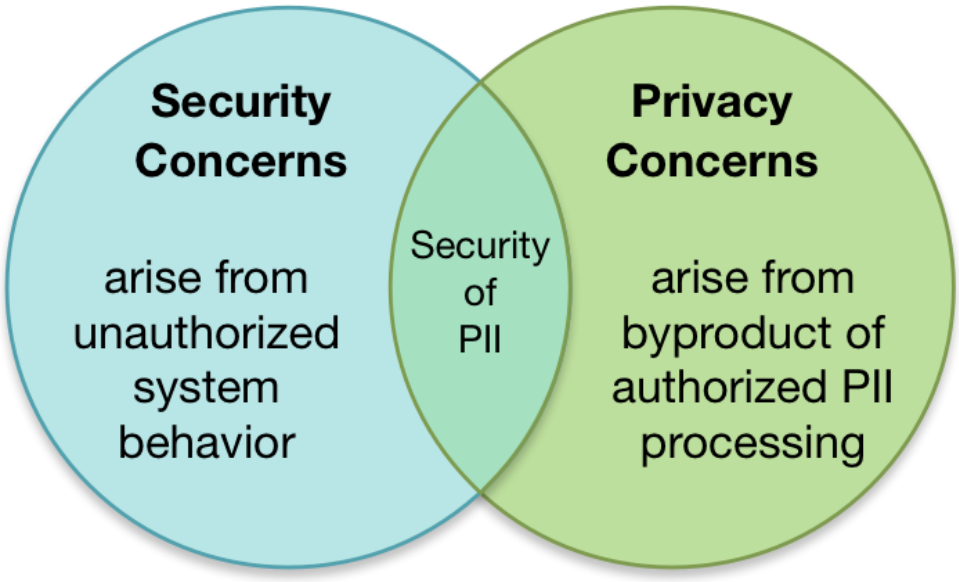

Figure 1. Relationship Between Information Security and Privacy.[10]

Figure two demonstrates that information security alone cannot guarantee privacy; therefore, systems must be engineered from their inception to address privacy concerns and ensure that the creation, collection, use, processing, retention, dissemination, or disclosure of personally identifiable information does not violate an individual's privacy.

B. ***Consequences of Privacy Violations***

The consequences of privacy violations must be understood to ensure organizations focus on the impact of privacy violations on the individual rather than merely legal and organizational economic consequences. The organization must be able to appropriately internalize the harm an individual faces rather than harm to the organization. The range of privacy problems faced by individuals is difficult to categorize; however, four general categories of problems would be loss of trust, loss of self-determination, discrimination, and economic loss.[11] When organizations and

[6] *Id.* at 7.
[7] *Id.* at 1.
[8] *Id.* at 7. The FIPPs are access and amendment, accountability, authority, minimization, quality and integrity, individual participation, purpose specification and use limitation, security, and transparency. *Id.*
[9] *Id.* at 8.
[10] *Id.*
[11] NISTIR 8062, AN INTRODUCTION TO PRIVACY ENGINEERING, *supra* note 1, at 10.

systems architects better understand the problems individuals face, the system's planners can begin able to operationalize systems that best protect against privacy risks.[12]

C. *Components of Privacy Engineering*

The FIPPs have endured and provided a necessary statement of organizational values systems must adopt to protect privacy; however, the FIPPs fail to provide necessary guidance for organizations to develop "a repeatable and measurable process that can be understood and communicated inside and outside the organization."[13] Privacy engineering does not seek to eliminate all privacy risks when an organization processes ePHI, elimination of all risk is impossible; however, privacy engineering seeks to establish a frame of reference where an outcome-based focus translates into system privacy requirements.[14]

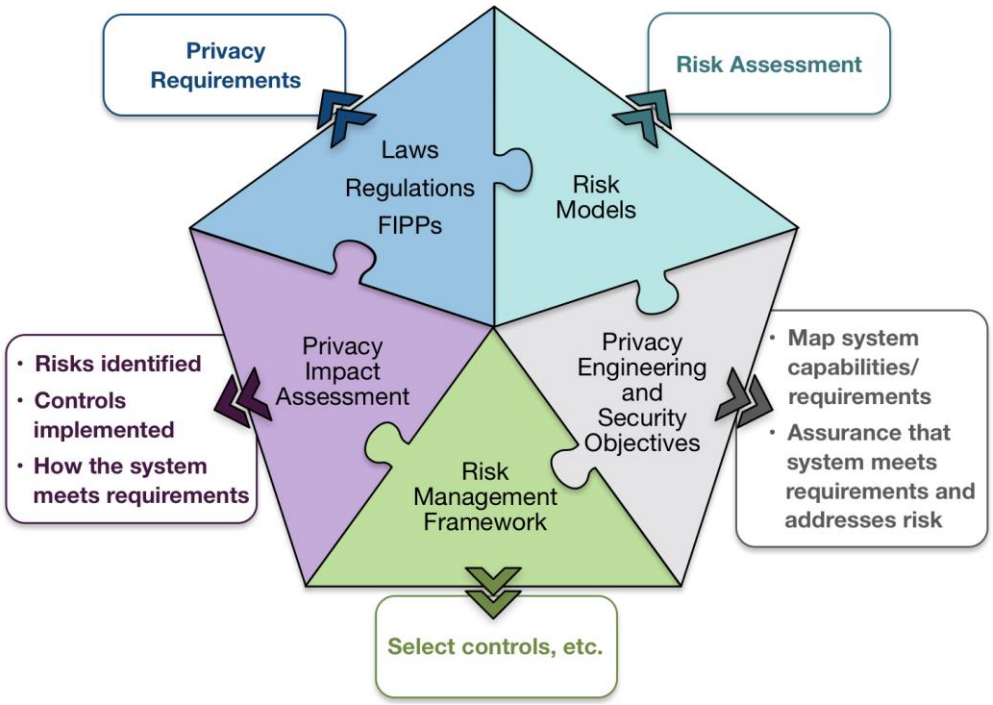

Figure 2. Components of Privacy Engineering.[15]

Figure three shows how existing materials and frameworks inform components of privacy engineering in order to coordinate and sequence organizational efforts to achieve consistent and measurable privacy improvising outcomes.[16] The internal parts of the pentagon demonstrate the existing materials and information. The statements within the boxes on the perimeter of the pentagon are components of privacy engineering.[17] The fact that several components of the figure

[12] *Id.* at 11.
[13] *Id.*
[14] *Id.* at 12.
[15] *Id.* at 15.
[16] *Id.*
[17] *Id.*

are borrowed from information security principles and practices highlights the fact that privacy and security complement one another.

Privacy requires trust. Privacy engineers must construct systems that provide sufficient measurable evidence to demonstrate sufficient levels of trustworthiness and obtain the benefits of medical interoperability.[18] A privacy engineer's tools are privacy engineering objectives, privacy risk models, privacy risk factors, and privacy risk characteristics.[19]

D. *Privacy Engineering Objectives*

Privacy engineering objectives are predictability, manageability, and disassociability.[20] NIST defines predictability as "enabling reliable assumption by individuals, owners, and operators about PII and its processing by an information system."[21] Manageability is defined as "providing the capability for granular administration of PII including alteration, deletion, and selective disclosure."[22] Disassociability is defined as "enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system."[23] The information security tirade, confidentiality, integrity, and availability, are used to achieve the security objective of privacy engineering. As stated previously, privacy engineering objectives are not intended to replace the FIPPS but provide a means to operationalize the values described in the FIPPS. Figure four below describes how the security engineering objectives align with the FIPPs.

[18] *See generally*, NISTIR 8062, AN INTRODUCTION TO PRIVACY ENGINEERING, *supra* note 1, at 16.
[19] *Id.*
[20] *Id.* at 17.
[21] *Id.*
[22] *Id.*
[23] *Id.*

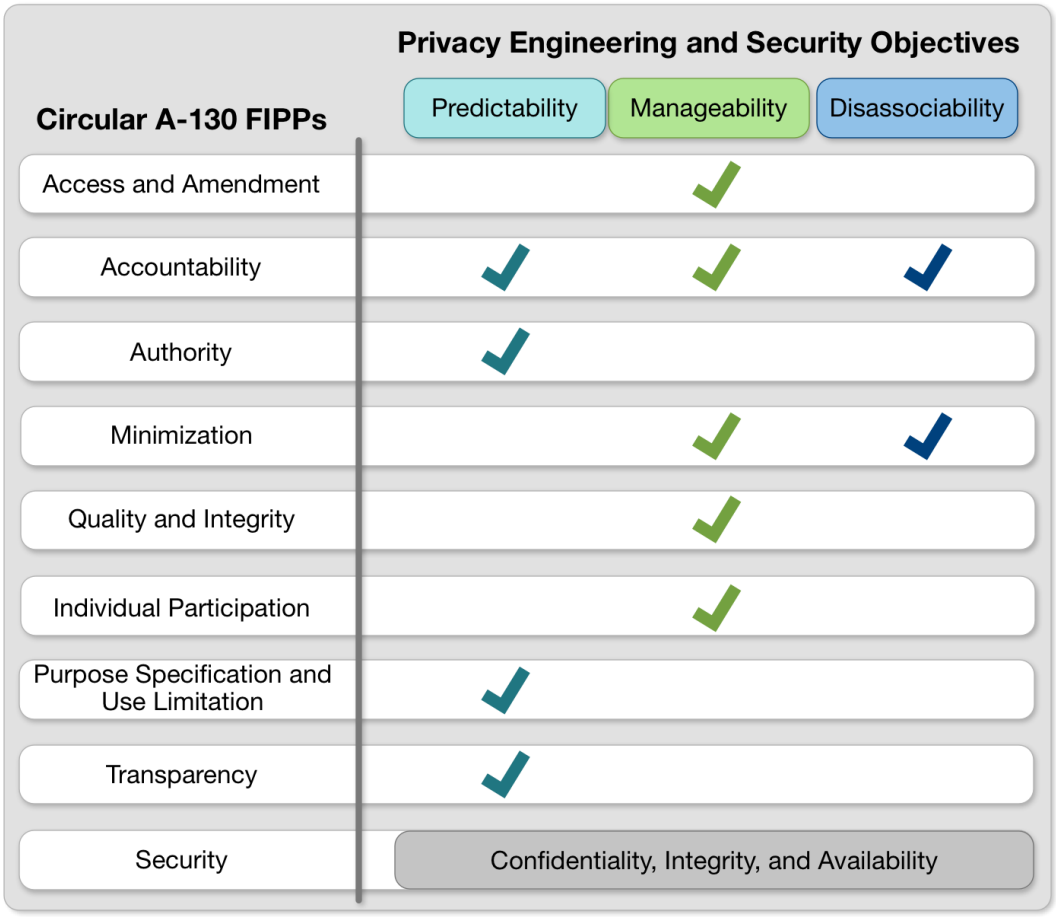

Figure 3. FIPPs and Privacy Engineering and Security Objectives[24]

The security engineering objective of predictability seeks to establish a reliable sense of what happens with PII after it enters a system, thereby supporting the FIPPs values of transparency and accountability.[25] Predictability is more than simple notice to patients of their privacy rights. Predictability seeks to ensure that patients make reliable assumptions about what happens to their data after it enters the system by determining whether or not patients understand the notice.[26] The notion of truly understanding what happens to ePHI after it enters a system also applies to stakeholders within the organization. In other words, internal stakeholders should never be surprised about what is happening to PHI after it enters their systems.[27]

Reliable assumptions by stakeholders, coupled with knowledge of the system, promote the value of transparency. Aligning notice with reliable assumptions about the system promotes a stable and trusting relationship between patients and the organizations receiving and processing

[24] NISTIR 8062, AN INTRODUCTION TO PRIVACY ENGINEERING, *supra* note 1, at 18.
[25] *Id.*
[26] *Id.*
[27] *Id.*

ePHI.[28] Additionally, reliable assumptions also enable innovation within the system by assessing the impact of any changes in processing following actual notice.[29]

Manageability is about enabling granular administration of an individual's information to promote the FIPPs values of access and amendment; accountability; minimization; quality and integrity; and individual participation.[30] A system would be considered manageable when data is administered in a manner that is consistent with an individual's privacy preferences, and the individual is treated fairly concerning the accuracy and transmission of information in the system.[31] Additionally, manageability should support data tagging, permission, and other metadata and identity management.[32]

The concept of disassociability recognizes that privacy risks exist in systems where authorized activity occurs where security concern of confidentially is no longer an objective.[33] Privacy engineers must evaluate systems and identify the points when the identity of an individual is not necessary for achieving the business objective.[34] The FIPPs value of data minimization is closely aligned with disassociability.[35] Privacy engineers must seek to utilize cryptographic techniques and other emerging technologies to complete transactions without associating the information with an individual.[36] Additionally, the cost of implementing technology or processes that enable disassociability must not prevent organizations from evaluating all available options; however, the cost-benefit analysis must inform the organization's privacy risk management strategy to ensure the system is optimized after all options are evaluated.[37]

E. ***Privacy Risk***

Privacy engineering must enable privacy risk management. The first step to properly manage privacy risk is to identify, model, and measure risk in a manner that enables privacy risks to be effectively managed throughout the enterprise.[38] Risk is the potential that an event will occur, causing an adverse impact on an individual or organization. The risk measure is typically a function of the adverse impacts expected to occur and the likelihood that the adverse event could occur.[39] Information security risk modeling utilizes the terms "threat" and "vulnerability" to describe risk in the context of data security.[40] However, information security is concerned about unauthorized activity in a system where privacy risk arises from authorized functions occurring in the system.[41] The NIST internal report recommends using the term "problematic data action" to describe "threats" for privacy risk assessment as to ensure the concept of "threat," as it is commonly understood in information security, is not dilute and forms the basis for additional confusion and

[28] NISTIR 8062, AN INTRODUCTION TO PRIVACY ENGINEERING, *supra* note 1, at 19.
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.* at 20.
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.* at 21.
[40] *Id.*
[41] *Id.*

miscommunication.[42] A problematic data action is "a data action that causes an adverse effect, or problem, for individuals."[43] Redefining threat as a problematic data action enables privacy engineers to consider various contextual factors when conducting a privacy risk assessment.

The privacy risk model uses the problematic data action to frame adverse events to assist organizations in identifying vulnerable systems and determining the likelihood and impact of a problematic data action.[44] The privacy risk model defines likelihood as "the probability that a data action will become problematic for a representative or typical individual whose PII is processed by the system."[45] The impact of a problematic data action is the magnitude of the harm caused by the data action.[46] The impact can be difficult for organizations to evaluate because only individuals can experience the impact of problematic data actions. Additionally, each individual may experience problems differently due to the types of harms caused by privacy risks, e.g., embarrassment or other psychologically based problems.[47] However, the NIST recommends that organizations use proxies to evaluate individual impact.[48] A few examples of proxies are legal compliance costs, mission failure if individuals do not trust the system, reputational cost, and employee morale or productivity.[49] Privacy engineering is not about eliminating all risk but enabling the organization to understand privacy risk better and avoid unacceptable consequences.[50]

Privacy risk is composed of three key characteristics: data actions, personally identifiable information (PII), and context. Data actions are with the organization does to process PII. Data processing can include disposal, collection, transfer, disclosure, transforming, generation, logging, and analysis.[51] The privacy engineer must work to identify the discrete data actions that occur in an organization's system and determine which actions could become problematic.[52] HIPAA defines the concept of PHI; however, privacy engineers should use a broad definition of PII to ensure they account for all ways an individual could be identified when information in the system is combined.[53] Context provides the information necessary for a privacy engineer to determine when the privacy boundary line has been crossed.[54] The circumstances surrounding an organization's processing of PII is context.[55] Context is the crucial factor an organization must evaluate to determine the likelihood that a data action will become a problematic data action and cause harm to an individual.[56]

[42] NISTIR 8062, AN INTRODUCTION TO PRIVACY ENGINEERING, *supra* note 1, at 21.
[43] *Id.*
[44] *Id.* at 21-22.
[45] *Id.* at 22.
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] *Id.* at 23.
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*

NIST FRAMEWORKS

Interoperability and the integrated clinical environment require the health care enterprise to manage risk, analyze risk, ensure privacy, and enforce security throughout the organization to include third-parties necessary to obtain and process data. The NIST provides the materials, frameworks, to build an enterprise health information system that is both private and secure.

A. *Risk Management Framework*

NIST special publication 800-37 revision 2 was released in December 2018. The updated version requires organizations to integrate privacy into the enterprise risk management framework, to assess risk in the supply chain, and to prepare for risk management throughout the system lifecycle properly.[57] The revision recognizes the importance of both information security and privacy:

> While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements. . . .[58]

NIST lists the seven major objectives of the revised Risk Management Framework (RMF):

1. Provide a closer linkage between risk management and C-suite;
2. Institutionalize critical risk management preparatory activities at all organizational levels;
3. Demonstrate how the NIST Cybersecurity Framework can be aligned with the RMF and implemented with NIST RMF processes;
4. Integrate privacy risk management process into the RMF to support privacy needs;
5. Promote the development of secure software and systems by aligning lifecycle-based systems with relevant tasks in the RMF;
6. Integrate security-related, supply chain risk management concepts into the RMF; and
7. Support both organization-generated and baseline control selection, and support the consolidated control catalog in NIST SP 800-53, Revision 5.[59]

Health care organizations must realize that managing privacy risk is a complicated matter that involves all echelons of the organization from the executive suites to the janitorial staff. Communication must be bi-directional to ensure that business objectives are effectively

---

[57] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUB. 800-37, REV. 2, RISK MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEMS AND ORGANIZATIONS (Dec. 2018), https://doi.org/10.6028/NIST.SP.800-37r2 [*hereinafter* NIST RISK MANAGEMENT FRAMEWORK].

[58] *Id.* at vi (*quoting* OFFICE OF MGMT. & BUDGET, CIRCULAR A-130, MANAGING INFORMATION AS A STRATEGIC RESOURCE (July 2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.).

[59] NIST RISK MANAGEMENT FRAMEWORK, *supra* note 57, at v.

communicated throughout the organization, and executives are adequately informed about the risks created by activities throughout the organization.[60] The enterprise's risk perspective must be broad, as shown in figure five below.

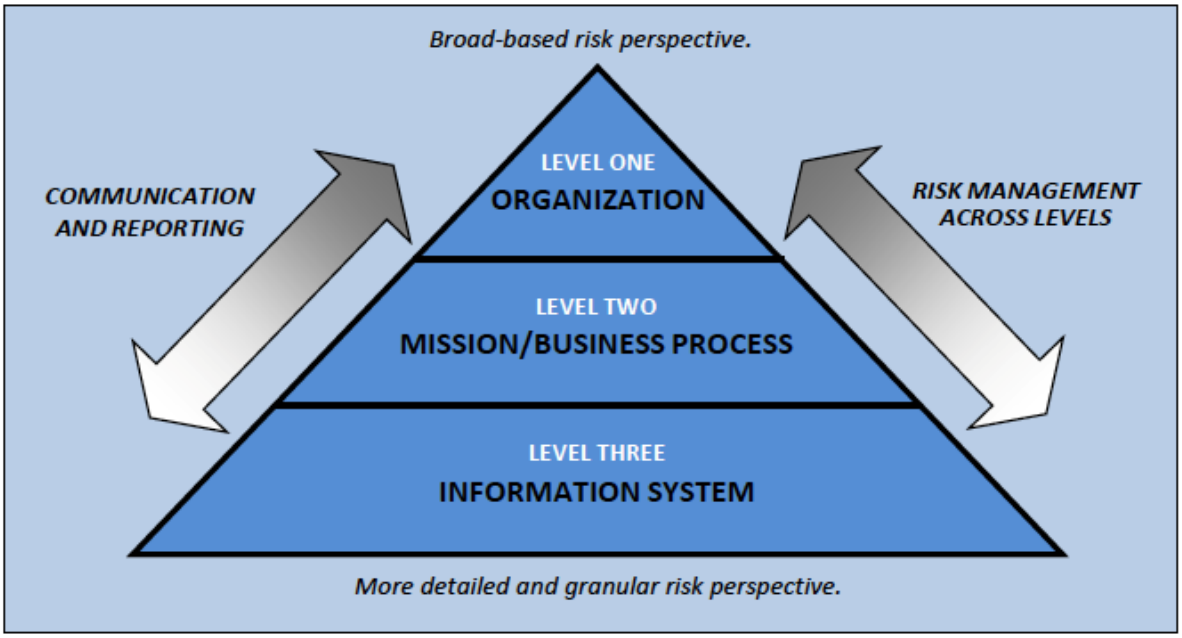

Figure 4. Organization-Wide Risk Management Approach.[61]

NIST 800-37 details seven steps in the Risk Management Framework.[62] The seven steps are:

> Prepare to execute the RMF from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
>
> Categorize the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.
>
> Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.
>
> Implement the controls and describe how the controls are employed within the system and its environment of operation.
>
> Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.

[60] NIST RISK MANAGEMENT FRAMEWORK, *supra* note 57, at 6.
[61] *Id.*
[62] *Id.* at 8.

> Authorize the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
>
> Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system. prepare, categorize, select, implement, assess, authorize, and monitor.[63]

When NIST revised 800-37 in December 2018, NIST added the prepare step as a key change to the risk management framework.[64] The primary objectives of the preparation phase were to facilitate effective organizational communication; facilitate identification of organization-wide common control baselines; reduce the complexity of IT systems and operations by promoting standardization; reduce the complexity of systems by eliminating unnecessary or redundant functions; and identify, prioritize, and focus resources on the organization's high-value assets.[65] The preparation phase of the NIST risk management framework enables organizations to engineer privacy and security into information systems and risk management processes enabling the organization to address new security and privacy issues as they arise. The prepare phase creates a foundation where organizations can build effective frameworks that address both privacy and security.

The NIST RMF system life cycle approach for security and privacy now consists of seven steps: prepare, categorize, select, implement, access, authorize, and monitor.[66] The addition of the "Prepare" step was a key change to the RMF. This change was incorporated into the RMF to "achieve more effective, efficient, and cost-effective security and privacy risk management processes."[67] The institutionalization of organization and system-level preparation can simply RMF execution, assist in the employment of innovative approaches to risk management, and increase automation for specifics tasks in the RMF.[68] If an organization does not engage in adequate preparation, security and privacy can become too costly, demand too many skilled professionals, and produce ineffective solutions.[69] The process of implementing RMF tasks will vary from organization to organization and may require the organization to diverge from the sequential order outlined in 800-37.[70] NIST 800-37, Appendix E, contains tables of the specific tasks associated with each step in the RMF, along with responsibilities and supporting roles.[71]

Privacy and security risk management processes complement one another but are not the same. "While many privacy risks arise from unauthorized activities that lead to the loss of confidentiality, integrity, or availability of PII, other privacy risks result from authorized activities involving the creation, collection, use, processing, storage, maintenance, dissemination,

[63] NIST RISK MANAGEMENT FRAMEWORK, *supra* note 57 at, 8-9.
[64] *Id.* at vi.
[65] *Id.* at vi-vii.
[66] *Id.* at ch. 3.
[67] *Id.* at vi.
[68] *Id.* at vi-vii.
[69] *Id.* at 8.
[70] *Id.* at 23.
[71] *Id.* app. E, at 126-38.

disclosure, or disposal of PII that enables an organization to meet its mission or business objectives."[72] The management of privacy risks requires specialized expertise and an understanding that communication regarding risk must occur throughout the organization.

The RMF recognizes the increasing need to manage risk in an organization's supply chain due to the increasing reliance on products, systems, and services provided by external providers.[73] In the context of the integrated clinical environment, the concept of interoperability dramatically increases privacy and security risk because health care institutions will be both suppliers and consumers of ePHI. Additionally, more vendors are likely to be involved, as the exchange of information will require complex information systems and necessary expertise that only a vendor can provide. Supply chain risks are often associated with an "organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed."[74] An organization must develop a supply chain risk management policy by coordinating efforts across the organization and building trust relationships between internal and external stakeholders.[75] Risk in the supply chain depends on the level of assurance the organization obtains from providers and the establishment of a chain of trust from external providers associated with privacy or security risks.[76]

B. *NIST Privacy Risk Analysis Methodology*

Privacy risk analysis is not well developed and could hinder the development of integrated clinical environments if not correctly addresses through a repeatable methodology. The NIST Privacy Risk Assessment Methodology (PRAM) provides a concrete method that health care organizations can adopt to analyze privacy risks systematically.[77] The PRAM consists of four worksheets: Framing Business Objectives and Organizational Privacy Governance, Assessing System Design and Supporting Data Map, Prioritizing Risk, and Selecting Controls.[78] When framing organizational objectives and privacy governance, the organization must evaluate the data processing environment to support the development of organizational privacy capabilities and trust in its data processing actions.[79] The second step in the PRAM is creating a data map of the systems data processing activities. The data map must include the data action, the data that is being processed by the system, and all relevant contextual factors related to data processing.[80] The next step in the PRAM is prioritizing risk, the most challenging part of the process. During risk prioritization, the likelihood and impact of each problematic data action that could occur in the

[72] NIST RISK MANAGEMENT FRAMEWORK, *supra* note 57, at 1.

[73] *Id.* at 20.

[74] *Id.*

[75] *Id.* at 20-21.

[76] *Id.* at 21-22.

[77] U.S. DEPT. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., PRIVACY ENGINEERING PROGRAM, RESOURCES, NIST PRIVACY RISK ASSESSMENT METHODOLOGY (Feb. 2019), https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources [*hereinafter* NIST PRIVACY RISK ASSESSMENT METHODOLOGY].

[78] *Id.*

[79] U.S. DEPT. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH, PRIVACY ENGINEERING PROGRAM, RESOURCES, NIST PRIVACY RISK ASSESSMENT METHODOLOGY: WORKSHEET 1: FRAMING ORGANIZATIONAL OBJECTIVES AND PRIVACY GOVERNANCE (Feb. 2019), https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

[80] U.S. DEPT. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH, PRIVACY ENGINEERING PROGRAM, RESOURCES, NIST PRIVACY RISK ASSESSMENT METHODOLOGY: WORKSHEET 2: SUPPORTING DATA MAP (Feb. 2019), https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

system is assessed to calculate a risk score for each data action.[81] The PRAM includes a Catalog of Problematic Data Actions and Problems to assist during the risk prioritization phase.[82] The final step in the PRAM is selecting controls. Controls are designed to mitigate the privacy risks identified in the previous steps to an acceptable level.[83] The PRAM is an iterative process that enables the organization to mature and become more risk-aware; however, the PRAM is only a single component to the privacy engineering.

C. *NIST Privacy Framework*

The NIST Privacy Framework is a collaborative effort between the NIST and public and private sector stakeholders to help organizations "identify and manage privacy risk to build innovative products and services while protecting individuals' privacy."[84] NIST released a discussion draft of the Privacy Framework in April 2019.[85] On 16 January 2020, the NIST release Version 1.0 of the NIST Privacy Framework.[86] Version 1.0 aligns with the NIST cybersecurity framework to promote organization efficiency in protecting PII while addressing unique privacy risks that arise for the collection, storage, use, and sharing of information necessary for an organization to achieve its business objectives.[87]

The NIST Privacy Framework consists of three parts: the cores, the profiles, and the implementation tiers.[88] The core "is a set of privacy protection activities and outcomes that allows for communicating prioritized privacy protection activities and outcomes across an organization from the executive level to the implementation/operations level."[89] The privacy activities and outcomes an organization seeks to achieve through the framework is considered a profile.[90] An implementation tier measures the progression of an organization's privacy risk management practices—informal and reactive to agile and risk-informed.[91]

---

[81] U.S. DEPT. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH, PRIVACY ENGINEERING PROGRAM, RESOURCES, NIST PRIVACY RISK ASSESSMENT METHODOLOGY: WORKSHEET 3: PRIORITIZING RISK (Feb. 2019), https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

[82] U.S. DEPT. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., PRIVACY ENGINEERING PROGRAM, RESOURCES, NIST PRIVACY RISK ASSESSMENT METHODOLOGY: CATALOG OF PROBLEMATIC DATA ACTIONS AND PROBLEMS (Feb. 2019), https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

[83] U.S. DEPT. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH, PRIVACY ENGINEERING PROGRAM, RESOURCES, NIST PRIVACY RISK ASSESSMENT METHODOLOGY: WORKSHEET 4: SELECTING CONTROLS (Feb. 2019), https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

[84] U.S. DEPT. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH, PRIVACY FRAMEWORK: ABOUT, https://www.nist.gov/privacy-framework (last visited Feb. 9, 2020).

[85] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., NIST PRIVACY FRAMEWORK: AN ENTERPRISE RISK MANAGEMENT TOOL, DISCUSSION DRAFT (Apr. 30, 2019), https://www.nist.gov/system/files/documents/2019/04/30/nist-privacy-framework-discussion-draft.pdf. [*hereinafter* DISCUSSION DRAFT: NIST PRIVACY FRAMEWORK]; Developing a Privacy Framework, 83 Fed. Reg. 56824, (notice, request for information Nov. 14, 2018).

[86] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0 (Jan. 16, 2020), https://www.nist.gov/document/nist-privacy-frameworkv10pdf [*hereinafter* NIST PRIVACY FRAMEWORK].

[87] *Id.*

[88] *Id.* at 2.

[89] *Id.*

[90] *Id.*

[91] *Id.*

In June 2019, the NIST proposed two possible cores, one core that was integrated with the NIST Cybersecurity Framework[92] and one that was separate and did not address the management of data security aspects of privacy risks.[93] Because an interoperable ICE implementation requires systems to be engineered to protect both security and privacy, the integrated core is best suited for the health care environment. The NIST adopted the integrated core in Version 1.0 of the Privacy Framework.[94] Figure five, below, demonstrates how the core functions of both the NIST Cybersecurity Framework and Privacy Framework can be used together to manage privacy and cybersecurity risks.

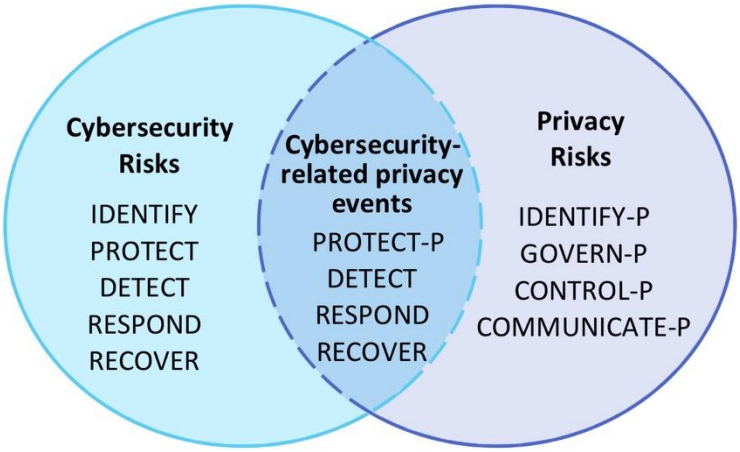

Figure 5. Using Functions to Manage Cybersecurity and Privacy Risks.[95]

The Privacy Framework consists of five core functions. The core functions are identify, govern, control, communicate, and protect.[96] The cores are defined as follows:

> IDENTIFY-P: Develop the organizational understanding to manage privacy risk for individuals arising from data processing.
>
> GOVERN-P: Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.
>
> CONTROL-P: Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.
>
> COMMUNICATE-P: Develop and implement appropriate

[92] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., SUPPLEMENTAL MATERIAL FOR NIST PRIVACY FRAMEWORK WORKSHOP #3, PROPOSED INTEGRATED CORE 1 (Jun. 26, 2019), https://www.nist.gov/system/files/documents/2019/06/26/pf-proposed-integrated-core-06.26.2019.pdf

[93] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., SUPPLEMENTAL MATERIAL FOR NIST PRIVACY FRAMEWORK WORKSHOP #3, PROPOSED SEPARATE CORE 1 (Jun. 26, 2019), https://www.nist.gov/system/files/documents/2019/07/03/pf-proposed-separated-core-06.26.2019.pdf

[94] NIST PRIVACY FRAMEWORK, *supra* note 86, at i.

[95] *Id.* at 7.

[96] *Id.* at 7.

> activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.
>
> PROTECT-P: Develop and implement appropriate data processing safeguards.[97]

The core functions of the Privacy Framework are used by an organization to manage privacy risks that arise from data processing.[98] Each core function is broken down into categories that describe privacy outcomes that are tied to activities and programmatic needs.[99] The categories are further distilled into subcategories that describe results that are necessary to support the outcomes and activities described in the core functions and categories.[100] Collectively, the core functions represent 100 distinct subcategories.[101] The NIST Privacy Framework provides a structured method to engineer a system to support privacy objectives, is structured in the same manner as the NIST Cybersecurity Framework, and is therefore designed to integrate the two complementarily frameworks to manage both security and privacy risks.

D. ***NIST Cybersecurity Framework***

The NIST created the Cybersecurity Framework (CSF) to provide a standard methodology to address cybersecurity.[102] The CSF aligns with the goals of the HIPAA Security Rule.[103] HHS has provided a crosswalk between the NIST CSF and the HIPAA Security Rule as an informative reference to enable organizations to understand better, manage, communicate cybersecurity risks.[104] The crosswalk does not ensure compliance or provide a safe harbor but assists security and privacy professionals in understanding how industry standards align with the HIPAA Security Rule.[105]

The CSF is organized in the same manner as the NIST Privacy Framework, cores, implementation tiers, and profiles.[106] The cybersecurity cores are:

> IDENTIFY (ID) – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
>
> PROTECT (PR) – Develop and implement appropriate safeguards

---

[97] NIST PRIVACY FRAMEWORK, *supra* note 86, at 7.

[98] *Id.* at 6.

[99] *Id.*

[100] *Id.*

[101] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., NIST PRIVACY FRAMEWORK, VERSION 1.0 CORE (Jan. 16, 2020), https://www.nist.gov/document/nist-privacy-framework-v10-core.

[102] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY Version 1.1. (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [*hereinafter* NIST CYBERSECURITY FRAMEWORK].

[103] U.S. DEP'T. OF HEALTH & HUMAN SERVS., OFFICE OF CIVIL RIGHTS, HIPAA SECURITY RULE CROSSWALK TO NIST CYBERSECURITY FRAMEWORK (Feb. 2016), https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.

[104] *Id.*

[105] *Id.*

[106] NIST CYBERSECURITY FRAMEWORK, *supra* note 102, at 7-8.

> to ensure delivery of critical services.
>
> DETECT (DE) – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
>
> RESPOND (RS) – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
>
> RECOVER (RC) – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.[107]

The CSF cores are subdivided in the same manner as the NIST Privacy Framework. When used together, the NIST CSF and NIST Privacy Framework enable organizations to efficiently engineer an information system that protects both privacy and security.

E. ***Integration of Security and Privacy Controls:***

The draft of NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organization, maps privacy to existing security controls already familiar to most cybersecurity professionals.[108] The Privacy Framework Core provides a map between the Privacy Framework's and Cybersecurity Framework's functions, categories, and subcategories to assist in integrating the management of privacy and security when necessary.[109] The NIST Cybersecurity Framework provides a map between the Cybersecurity Framework and the security controls in NIST Special Publication 800-54, Revision 4.[110]

A health care enterprise implementing an integrated clinical environment must manage its risk by integrating privacy and security controls at the points in the enterprise where the disciplines converge.[111] The NIST Risk Management Framework, Privacy Risk Assessment Methodology, Privacy Framework, and Cybersecurity Framework provide the necessary building blocks to construct an enterprise system that is both private and secure. However, the NIST frameworks and methodology must be placed within and integrating architecture.

CONCLUSION

In Security and Privacy of the Integrated Clinical Environment Part II, the discipline of privacy engineering was discussed along with the objectives of privacy engineer and the definition of privacy risk. Following the discussion of privacy engineering, the NIST Privacy Framework, Cybersecurity Framework, Risk Management Framework, and Privacy Risk Analysis Methodology were reviewed to demonstrate how these NIST tools are aligned and could be used

---

[107] NIST CYBERSECURITY FRAMEWORK, *supra* note 102, at 7-8.

[108] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., DRAFT NIST SPECIAL PUB. 800-53 REV. 5, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS (draft Aug. 2017), https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf [*hereinafter* NIST SECURITY AND PRIVACY CONTROLS].

[109] U.S. DEP'T. OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., NIST PRIVACY FRAMEWORK, VERSION 1.0 CORE (Jan. 16, 2020), https://www.nist.gov/document/nist-privacy-framework-v10-core.

[110] NIST CYBERSECURITY FRAMEWORK, *supra* note 102, at 24 – 44.

[111] NIST SECURITY AND PRIVACY CONTROLS, *supra* note 108; NIST RISK MANAGEMENT FRAMEWORK, *supra* note 57; NIST PRIVACY FRAMEWORK, *supra* note 86; NIST CYBERSECURITY FRAMEWORK, *supra* note 102, at 7-8.

to manage privacy and security in an interoperable, ICE throughout the enterprise. Part III of this article will discuss how the Sherwood Applied Business Security Architecture (SABSA) can be used to integrate the frameworks and methodologies presented in Part II into an enterprise architecture to ensure an organization deploying an interoperable, ICE is compliant with their obligation to protect the privacy and security of a patient's health information.