NIST Privacy Framework: Protecting Privacy While Promoting Interoperability

Save to myBoK

By Karen Starling Greenhalgh, HCISPP, CHC, CHPC

Privacy is often seen as a barrier to electronic health information exchange (HIE). To help address those concerns and meld core privacy principles with proven oversight and accountability mechanisms, the National Institute of Standards and Technology (NIST) is scheduled to release the Privacy Framework: An Enterprise Risk Management Tool this month. Draft versions are also available for review.[1] Designed with collaboration between NIST, healthcare industry leaders, and privacy experts, the NIST Privacy Framework provides healthcare providers with an effective approach to protecting the privacy of the individual while implementing complex new interoperability and patient access programs.

Because HIE is a such a high priority, the Centers for Medicare and Medicaid Services (CMS) encouraged implementation of electronic health record (EHR) technology throughout the US healthcare delivery system by instituting the meaningful use (MU) EHR Incentive Program.[2] While MU was successful with respect to industry-wide adoption of EHRs, it opened the door to unexpected security risks. In 2018, CMS revamped MU by renaming it the Promoting Interoperability (PI) program, emphasizing a broader focus on interoperability and improving patient access to health information.[3] However, the privacy and security issues remain.

Privacy in Healthcare

Individuals' privacy is of particular importance to healthcare providers because their patients' well-being depends upon their ability to share personal data. Loss of trust could make a patient hesitant to share critical information or reluctant to pursue necessary medical care.

There have been numerous attempts to address privacy issues in healthcare that are of interest to health information management (HIM) professionals. For example, the government defined Fair Information Practice Principles (FIPPs) as part of the Privacy Act of 1974.[4] FIPPs set forth eight key principles that formed the backbone of privacy law in the United States and are recognized by healthcare privacy professionals.

In 2008, the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (Privacy and Security Framework) was released by the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC).[5]

The ONC's Privacy and Security Framework also comprises eight principles that are derived from FIPPs.

Figure 1 (below) exhibits the privacy principles stated in the FIPPs and ONC's framework. These are similar and provide a good foundation, but as value statements they are difficult to operationalize.

Figure 1: Privacy Principles

FIPPs	ONC Privacy and Security Framework

1. Transparency 2. Individual participation 3. Purpose specification 4. Data minimization 5. Use limitation 6. Data quality and integrity 7. Security 8. Accountability	1. Individual access 2. Correction 3. Openness and transparency 4. Individual choice 5. Collection, use, and disclosure limitation 6. Data quality and integrity 7. Safeguards 8. Accountability

In 2015 ONC issued the Guide to Privacy and Security of Electronic Health Information.[6] This guide refers to the importance of privacy and security and offers guidance on implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, but does not address the Privacy Rule. Security is necessary to protect the privacy of individuals, but security alone cannot address all privacy issues.

The Privacy and Security Connection

Privacy professionals understand the importance of protecting privacy, but many in the healthcare industry are confused when differentiating between privacy and cybersecurity. As cybersecurity becomes more established, privacy is often simplified to an outcome of an effective cybersecurity program. In order to promote interoperability and access while protecting the privacy of individuals, the differences between privacy and cybersecurity must be clearly defined.

While the term "privacy" is frequently used, there is no universally accepted definition of the word. Privacy's scope, meaning, and value can be complex and confusing. To help understand privacy, consider that it is primarily used to answer the following questions:

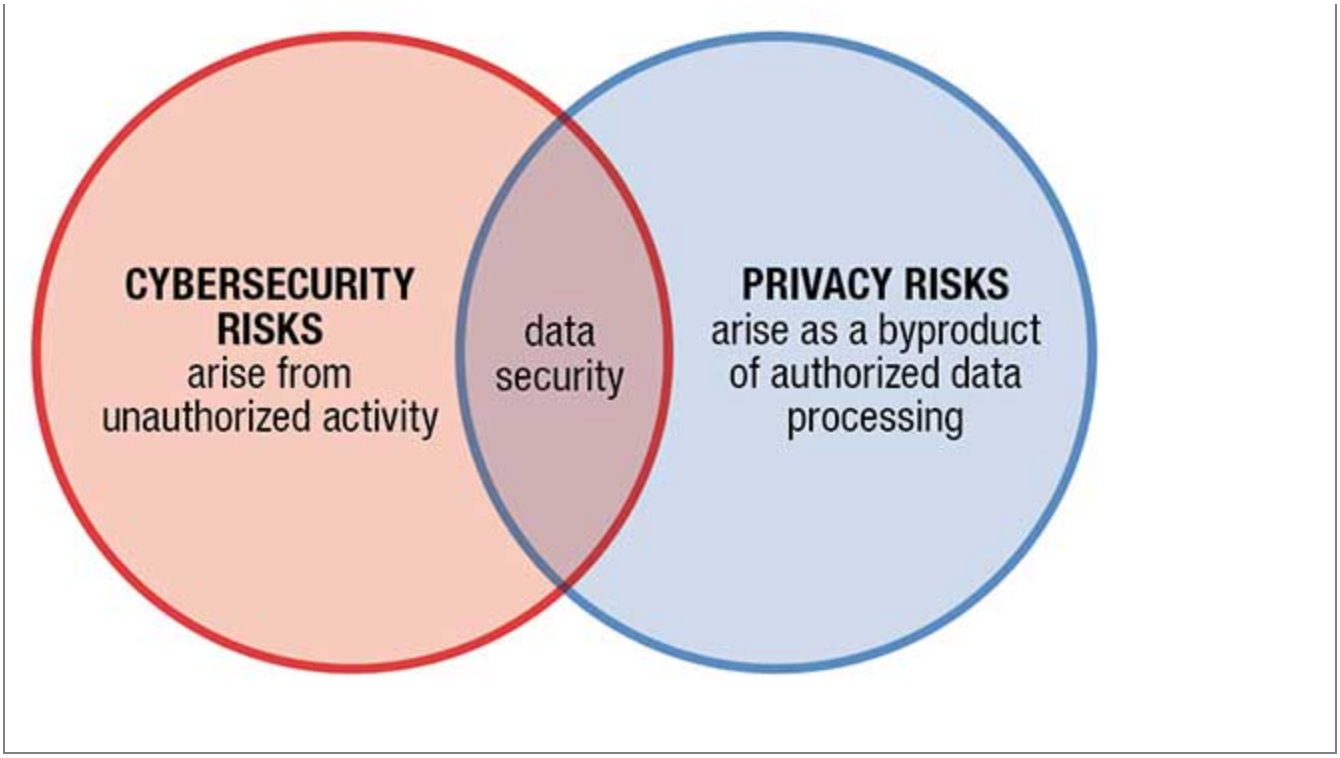
- Who has access to personal information and under what conditions?
- Which data can be collected?
- How is personal information collected, stored, and used?
- What are the justifications, if any, for data collected for one purpose and then reused for a second purpose?
- Has an individual authorized particular use of his or her personal information?

The term "security" is more tangible and therefore more easily understood. It can be defined as the procedural and technical measures required to:

- Prevent unauthorized access, modification, use, or dissemination of data stored or processed in a computer system
- Prevent any deliberate denial of service
- Protect the system in its entirety from physical harm

When someone hacks into a computer system, there is a breach of security and, potentially, a breach of privacy. No security measure, however, can prevent invasion of privacy by those who have authority to access the record. Comprehensive data security requires mitigation of both security risks and privacy risks, as illustrated in Figure 2 (below).

Figure 2: Cybersecurity and Privacy Risk Relationship



Privacy and Security Risk

The new NIST Privacy Framework offers a fresh approach to privacy management. By applying an outcome-based methodology to recognized privacy value statements, the NIST framework approaches privacy as a manageable risk. This approach, based on the widely accepted NIST Cybersecurity Framework (CSF),[7] enables privacy compliance practitioners to state goals and achieve a measurable outcome for individuals' privacy. Approaching privacy as a risk, NIST applied their proven standards for identifying and managing security risks to develop guidelines for risk-based privacy management.

Aligning privacy risk and security risk to increase protection of health information systems will bolster trust in such systems and promote their adoption. While the NIST framework is designed to function as a standalone tool or in conjunction with any cybersecurity program, it is also specifically designed to work with the CSF. Both NIST frameworks are based on risk models that define the risk factors to be assessed, and the relationships among those factors.

Security Risk Model

The NIST Security Risk Model, based on the widely known CIA Security Triad, is focused on unauthorized activity creating a security risk, impacting confidentiality, integrity, or availability of information or systems.

The key aspects of the CIA Security Triad are confidentiality, integrity, and availability:

- **Confidentiality:** preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- **Integrity:** guarding against improper information modification or destruction; includes ensuring information nonrepudiation and authenticity
- **Availability:** ensuring timely and reliable access to and use of information

Security risk factors to take into account when developing security risk models include:

- Threat

- Vulnerability
- Likelihood
- Impact

Privacy Risk Model

The NIST Privacy Risk Model is focused on authorized processing (planned and permissable) of personally identifiable information (PII) and protected health information (PHI) that creates a privacy risk, which impacts predictability, manageability, and disassociability. NIST introduced the concept of privacy risk in a report titled "An Introduction to Privacy Engineering and Risk Management in Federal Systems."[8] The report proposes the idea of a "PMD" Privacy Triad focusing on predictability, manageability, and disassociability:

- **Predictability:** Enabling reliable assumptions by individuals, owners, and operators about PII/PHI and its processing by an information system
- **Manageability:** Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure
- **Disassociability:** Enabling the processing of PII or events without association to individuals or devices beyond the operations requirements of the system

Privacy risk factors to take into account when developing privacy risk models include:

- Likelihood
- Problematic data action
- Impact

Problematic data actions are issues caused by authorized processing of PII/PHI. These problems may be less visible than a security event or not as well understood but can result in real consequences. NIST describes them as ranging from dignity-type losses—embarrassment, stigmas, or discrimination—to more tangible harms such as economic loss or physical harm.[9] The Privacy Framework identifies nine problematic data actions:

1. Appropriation
2. Distortion
3. Induced disclosure
4. Insecurity
5. Reidentification
6. Stigmatization
7. Surveillance
8. Unanticipated revelation
9. Unwarranted restriction

A Powerful Tool for HIM

Application of NIST's extensive work concerning security and privacy risk management into the Privacy Framework has created a powerful tool for health information management. Privacy experts understand data security and data privacy are not the same but share many objectives. Both are required for comprehensive data security. The NIST Privacy Framework methodology of assessing privacy with a risk-based and outcome-based approach, in alignment with the NIST CSF, will allow healthcare entities to align privacy and security while incorporating interoperability and patient access requirements.

Notes

1. National Institute of Standards and Technology. Privacy Framework. https://www.nist.gov/privacy-framework.
2. Centers for Disease Control and Prevention. "Public Health and Promoting Interoperability Programs (formerly known as Electronic Health Records Meaningful Use)." Last accessed 8/9/19. https://www.cdc.gov/ehrmeaningfuluse/introduction.html.
3. Centers for Medicare and Medicaid Services. "Promoting Interoperability (PI)." Last accessed 8/9/19. https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html.
4. Department of Homeland Security. "Privacy Policy Guidance Memorandum." Last accessed 8/10/19. https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-01_0.pdf.
5. Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information." Last accessed 8/10/19. https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf.
6. Office of the National Coordinator for Health Information Technology, "Guide to Privacy and Security of Electronic Health Information." Last accessed 8/10/19. https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.
7. National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1." Last accessed 8/10/19. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
8. National Institute of Standards and Technology. "NISTIR 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems." Last accessed 8/10/19. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.
9. National Institute of Standards and Technology. "Privacy Risk Assessment Methodology (PRAM), update released 2019, Catalog of Problematic Data Actions and Problems." ZIP file download. Last accessed 8/10/19.https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

Karen Starling Greenhalgh (Karen@CyberTygr.com) is founder and managing principal of Cyber Tygr.

Article citation:
AHIMA. "NIST Privacy Framework: Protecting Privacy While Promoting Interoperability" *Journal of AHIMA* 90, no.90 (September 2019): 32-33, 43.