THE 405(d) POST

VOLUME VI

HHS 405(d)
Aligning Health Care Industry Security Approaches

The NIST Privacy Framework

By Karen Greenhalgh, HCISPP, CHPC, CHC, 405(d) Task Group Member

Since the Cybersecurity Act of 2015 (CSA), cybersecurity is often considered to be the solution for protecting privacy. The healthcare industry, contending with HIPAA and increasing privacy regulation, is recognizing that cybersecurity and compliance programs are not structured to meet privacy needs. While good information security practices help manage privacy risk, those measures alone are not sufficient to address the full scope of privacy risks. The NIST Privacy Framework is designed to bridge the gap between information security and individual privacy, illustrated in Figure 1.

Recognizing the boundaries and overlap between privacy and security is key to determining when existing security-focused guidance may be applied to privacy concerns and illuminating gaps that need to be filled to achieve data security. For example, existing information security guidance does not address the consequences of an inadequate consent mechanism for use of PII/PHI, what PII/PHI is being collected, or which changes in use of PII/PHI are permitted by authorized personnel. Entities cannot effectively manage privacy solely based on managing security. Reducing cybersecurity risks by preventing unauthorized access will protect privacy but cannot protect against privacy risks which arise from authorized activity.

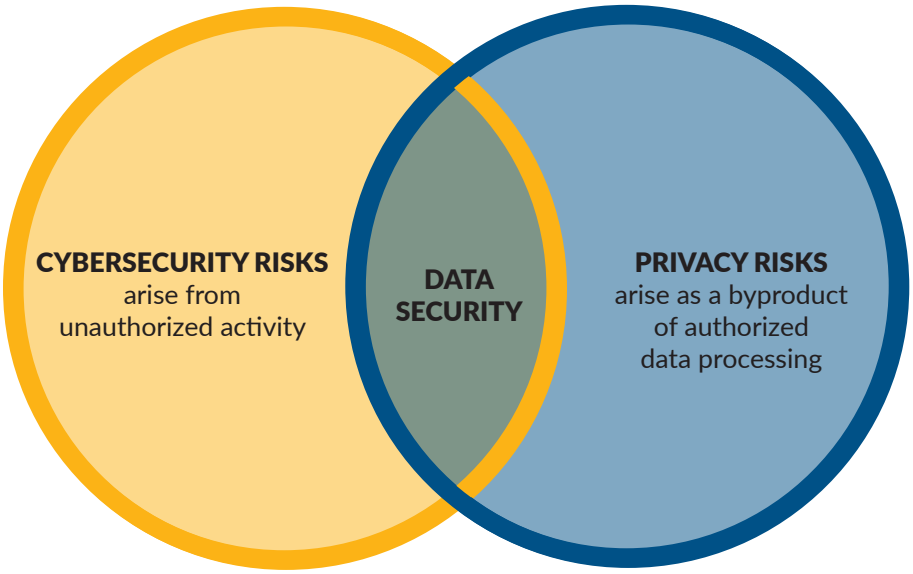

FIGURE 1: NIST Privacy Framework Discussion Draft issued April 30, 2019 NIST Privacy Framework Discussion Draft issued April 30, 2019[1]

Cybersecurity risks arise from unauthorized activity

Through social engineering, a bad actor could trick an employee into revealing login and password for

the billing department, allowing the bad actor to divert patient payments. This cyberattack is a potential privacy breach due to unauthorized access which could expose patient information.

Unprotected medical devices may allow access into an entire network, placing data at risk of being compromised.

Privacy risks which occur because of unauthorized activity may be mitigated by cybersecurity practices.

Privacy risks arise from authorized activity

Use and disclosure of PHI is strictly regulated; the Privacy Framework helps organizations manage the privacy risk of an impermissible use or disclosure. For example, suppose hospital staff, with permission to access the data, share private information with the news media about a patient who happens to be famous?

Another example is a recent case investigated by OCR. One patient filed a complaint after receiving a hospital bill containing another patient's PII. OCR's investigation determined over 500 patients had their billing information merged with that of other patients. Though the bills only contained names, account numbers, and dates of service, OCR determined this was a privacy breach.

Privacy risks which occur because of authorized activity may not be prevented by cybersecurity practices.

Security Risk and Privacy Risk Management

The NIST Privacy Framework functions as a stand-alone tool but is specifically designed to work with the NIST Cybersecurity Framework (CSF). The CSF is so widely embraced by the healthcare industry that OCR released a crosswalk relating the HIPAA Security Rule with the CSF. A similar crosswalk aligning the Privacy and Breach Notification Rules with the NIST Privacy Framework is under consideration.

NIST has developed guidelines for risk-based privacy management by applying their widely accepted standards for identifying and managing security risks. NIST's security and privacy risk models define the risk factors to be assessed, and the relationships among those factors.

NIST Security Risk Model[2]

The Security Risk Model is focused on unauthorized activity creating a security risk, resulting in loss of confidentiality, integrity, or availability of information or systems, the familiar CIA Security Triad.

The Security Triad

- 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 non-repudiation and authenticity

- Availability: ensuring timely and reliable access to and use of information

Security Risk Factors
- Threat
- Vulnerability
- Likelihood
- Impact

NIST Privacy Risk Model[3]

The Privacy Risk Model is focused on authorized processing of PII/PHI (planned and permissible) creating a privacy risk, resulting in loss of **p**redictability, **m**anageability, or **d**isassociability, NIST's **PMD** Privacy Triad.

The Privacy Triad
- 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:
- Likelihood
- Problematic data action
- Impact

Application of NIST's extensive work concerning security and privacy risk management into an operational privacy framework has created a powerful tool, as illustrated in Figure 2. 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, allows healthcare entities to incorporate privacy and security into their enterprise risk management program. Designed with collaboration between NIST and healthcare industry leaders, the NIST Privacy Framework is a tool that may bridge the gap between security and privacy.

FIGURE 2

If you would like to learn how HICP maps to other frameworks like the NIST Cybersecurity framework click below to check out our new Threat Mitigation Matrix!

CLICK HERE FOR THREAT MITIGATION MATRIX

[1] NIST Privacy Framework: An Enterprise Risk Management Tool, Discussion Draft issued April 30, 2019. https://www.nist.gov/system/files/documents/2019/04/30/nist-privacy-framework-discussion-draft.pdf#page=6
[2] FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
[3] National Institute of Standards and Technology (NIST) IR 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems, Appendix F, January 2017. https://bit.ly/33SdkfV

405(d) In the Spotlight

Network Management

As the healthcare workforce and technology become more remote and complex, it is important for organizations of all sizes to protect their networks from cyber threats. Computers communicate with other computers through networks. These networks are connected wirelessly or via wired connections (e.g., network cables), and networks must be established before systems can interoperate. Networks that are established in an insecure manner increase an organization's exposure to cyberattacks. Proper cybersecurity hygiene ensures that networks are secure and that all networked devices access networks safely and securely. Even if network management is provided by a third-party IT support vendor, the organization must understand key aspects of proper network management and ensure that they are included in contracts for these services.

One of the best ways to protect your organization's network is through network segmentation. Network segmentation restricts access between devices to that which is required to successfully complete work. This will limit any cyberattacks from spreading across your network. To apply network segmentation in your organization consider the following tips below:

- Disallow all Internet bound access into your organization's network. If you host servers that interface with the internet, consider using a third-party vendor who will provide security as part of the hosting service.
- Restrict access to assets with potentially high impact in the event of compromise. This includes medical devices and internet of things (IoT) items (e.g., security cameras, badge readers, temperature sensors, building management systems).
- Just as you might restrict physical access to different parts of your medical office, it's important to restrict the access of third-party entities, including vendors, to separate networks. Allow them to connect only through tightly controlled interfaces. This limits the exposure to and impact of cyberattacks on both your organization and on the third-party entity.
- Establish and enforce network traffic restrictions. These restrictions may apply to applications and websites, as well as to users in the form of role-based controls. Restricting access to personal

websites (e.g., social media, couponing, online shopping) limits exposure to browser add-ons or extensions, in turn reducing the risk of cyberattacks.

Protecting our patients from cyber threats even in these uncertain times is paramount to keeping our healthcare systems running smoothly and securely. For more information on network segmentation and other ways to protect your organization from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

Happening Around Us

Phishing campaign targets remote healthcare workers with fake voicemail notifications

SM Magazine

SC Media reports that cyber attackers looking for new angles to socially engineer employees working from home under COVID-19 conditions have devised a new phishing campaign that distributes emails that look as if they were generated by Private Branch Exchange (PBX), a legacy technology that integrates with employees' email clients so they can receive their voicemail recordings. Ironscales reported that the operation, discovered by its researchers last month, has threatened nearly 100,000 mailboxes around the world, reaching enterprises across multiple sectors. PBX is a useful tool for employees who lack convenient access to their office landlines. Aware of this, malicious actors are now crafting email subject lines designed to trick recipients into thinking they have received a new voice message. In some cases, the phishing actors use highly targeted subject lines that include a specific company's or person's name, according to the blog post authored by Vice President of Pre-Sales Engineering/Director of Engineering – Americas Ian Baxter. The sender's name is also customized for the target. Ironscales notes that since the emails do not bear an actual malicious payload that might trigger a detection, the emails can bypass secure email gateways and eludes the DMARC authentication protocol. Because the healthcare workforce is even more remote today it is imperative that good cyber hygiene be used in identifying these attacks. To learn more about how to protect your organization from cyber threats check out Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

New Report Shows Health Sector Most Targeted by Hackers in 2019

Health IT Security

HealthITSecurity reports that the healthcare sector was the most targeted sector by hackers and cyberattacks in 2019. And its 382 data breaches cost the sector more than $17.76 billion, according to ForgeRock's 2019 Consumer Breach Consumer Breach Report. The healthcare sector accounted for 45 percent of data breaches in 2019, followed by the banking, insurance, and financial sector at 12 percent. Researchers calculated the $17.76B spent on data breaches amounted to about $429 per breached patient record, up 5.14 percent from 2018. ForgeRock researchers analyzed the data breaches affecting consumers across all sectors reported between January 1, 2019 and March 31, 2020, which were the categorized by sector. Researchers found that breaches have dramatically increased during that timeframe, both in numbers and in costs. In fact, the average cost of a single breach increased 112 percent from $3.86 million in 2018, to $8.9 million in 2019. The number of breaches impacting consumers rose 78.57 percent, from 2.8 billion in 2018, to 5 billion in 2019. To learn more about how to protect your organization from cyber threats check out Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

Enterprise Mobile Phishing Attacks on the rise amidst COVID-19 Pandemic

Threat Post

ThreatPost reports the rate of mobile phishing rose sharply by 37% between the last quarter of 2019 and the first quarter of 2020, a boost most likely due to the increased number of people working from home due to COVID-19 stay-at-home orders, new research has found. In fact, encounter rates for enterprise mobile phishing increased 37 percent between the last quarter of 2019 and the first quarter of 2020, from around 16 percent to 22 percent. The Mobile Phishing Spotlight Report from Lookout highlights how threat actors have shifted their tactics to take advantage of the evolving move from the physical to mobile or home office in the wake of the COVID-19 pandemic, which forced many companies to order their employees to work from home and use mobile devices as part of their every-day productivity. As this trend will likely continue for the foreseeable future — with large corporations such as Google, Twitter, Facebook and Amazon keeping their workforce remote until all shelter-in-place regulations are lifted — organizations may have to shift their security tactics and education of employees to keep up with the evolving threat. This also affects the healthcare community as telehealth and other services and employees have become more remote. To learn more about how to protect your organization from cyber threats check out Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

405(d) Events and Announcements!

405(d) Spotlight Webinar: August 26 at 1:00 p.m.

Additional Resources

Fake Online Coronavirus Map Alert

Access Control for Health Information Systems

Citric Vulnerabilities and APT 41 Whitepaper

Telehealth Remote Communications Guidance

Happening Around Us Sources

1. SM Magazine
2. Health IT Security
3. Threat Post

About The 405(d) Post

This newsletter is for information purposes only and aims to broaden awareness and align healthcare security approaches. The news articles represented in this newsletter are chosen at random to foster awareness and are not in promotion of any news organization. The "A Word from the Task Group" is written by a different 405(d) Task Group Member each issue and does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute to this newsletter.

Need To Contact Us? Email us at cisa405d@hhs.gov