The NIST Privacy Framework: An enterprise risk management tool

compliancecosmos.org/nist-privacy-framework-enterprise-risk-management-tool

By Karen Greenhalgh, HCISPP, CHC, CHPC

Karen Greenhalgh (karen@cybertygr.com) is Managing Principal and Founder of Cyber Tygr in Virginia Beach, VA.

linkedin.com/in/karen-greenhalgh

Protecting the privacy rights of individuals has become a primary goal of governments and organizations around the globe. In the U.S., Congress is considering an American version of the EU's General Data Protection Regulation (GDPR), and the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule is under scrutiny. The healthcare industry, still struggling with HIPAA and facing increasing privacy regulation, is recognizing that current cybersecurity and compliance programs are not structured to meet privacy needs. But how is the privacy of individuals to be effectively managed? By applying outcome-based methodology, the new National Institute of Standards and Technology (NIST) Privacy Framework treats privacy as a manageable risk.[1] This approach to privacy enables privacy compliance practitioners to state goals and achieve a measurable outcome for individuals' privacy.

An enterprise risk management tool

Scheduled for release in October 2019, the NIST Privacy Framework is the two-year culmination of intensive work by privacy experts from across the nation's public and private sectors, many from the healthcare industry. Representation by healthcare industry leaders in the creation of the Privacy Framework assures the framework will address the full scope of privacy risk. As an enterprise risk management tool, the Privacy Framework will help organizations answer the fundamental question: How are we considering the direct privacy impacts to individuals, and the secondary impact to the organization, as we develop our systems, products, and services?

Privacy vs security: Laws and regulations

Information security laws and regulations typically require risk analyses or other specific actions to assess effectiveness and allow flexibility in how controls are implemented. In contrast, privacy laws and regulatory policies typically prescribe precise obligations an organization must follow. This fixed approach to privacy produces assessments focused on compliance as rule enforcement, with less attention to measuring effectiveness of achieving a positive outcome for privacy. For example, assessments are conducted to determine

whether the HIPAA-required Notice of Privacy Practices (NPP) exists, without an assessment to evaluate whether people are likely to read that notice and receive some privacy-protective benefit.

Comparing HIPAA's Security and Privacy Rules provides an example of the difficulties created by obligation-based privacy regulations.

Security Rule

- Section 164.306: Security standards: General rules. "(b) Flexibility of approach. (1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in the sub-part."[2]
- Entities are also required to perform outcome-based activities, including risk analyses, technical assessments, and non-technical assessments.

Privacy Rule

- Federal Register, page 82471: "This rule establishes national minimum standards to protect the privacy of individually identifiable health information in prescribed settings."[3]
- Section 164.520 details the Privacy Rule's NPP for Protected Health Information (PHI), and is an example of obligation-based rigidity. This five-page section has the word "must" 26 times referring to covered entities, with no "flexibility of approach."[4]

Privacy regulations vs. security regulations

The result of enforcing privacy regulations without clear goals to measure progress is perfectly illustrated by the Office for Civil Rights (OCR) and the Department of Health and Human Services (HHS). In December 2018, the OCR/HHS issued a Request for Information on Modifying HIPAA Rules to Improve Coordinated Care.[5]

Of the 54 multi-part questions, 11 pertain to NPP because "OCR has received anecdotal evidence that individuals are not fully aware of their HIPAA rights" (which is the understood intent of the notification section of the Privacy Rule). The five-page NPP section of the Privacy Rule issues detailed rules for writing and distribution of the NPP to patients. Compliance practitioners are required to assure the myriad details in those five pages are executed. However, there is no requirement to assess comprehension by patients—the actual intent of the regulation.

Consider the outcome-based approach from using the Privacy Framework. The working draft at the time of this writing includes two subcategories: CM.AW-P1 would apply to the

writing and distribution of the NPP, and CM.AW-P2 provides a measurable outcome-based action, rather than a check-the-box action:

- CM.AW-P1: Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
- CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risk are established and in place.

The healthcare industry needs a Privacy Framework

The healthcare industry faces an ongoing challenge to design, operate, or use technologies in ways that consider diverse privacy needs. Constantly emerging cutting-edge technologies such as Internet of Things (IoT) and artificial intelligence (AI) continue to raise new concerns. Although good cybersecurity practices help manage privacy risk by protecting information, those measures alone are not sufficient to address the full scope of privacy risks. Privacy risks arise as organizations collect, store, use, and share information to meet their mission, as well as how individuals interact with products and services.

Privacy professionals recognize the Fair Information Practice Principles (FIPPs)[6] as foundational principles for handling personally identifiable information (PII) and PHI, and in developing baseline considerations for protecting the privacy of individuals. As value statements, FIPPs are difficult to operationalize. Assessing and analyzing privacy risk require a well-articulated set of privacy objectives, allowing a privacy risk assessment and development of detailed implementation requirements that are practical and actionable. Stating measurable, agreed-upon outcomes creates a clearly defined goal that can be understood at all organizational levels of an enterprise. This is the purpose of the Privacy Framework.

Relevance of NIST Privacy Framework to healthcare

Privacy has a heightened importance in healthcare. Our clients are patientswho must be able to trust their healthcare providers to protect their most personal data. Concerns about privacy can cause a loss of trust with two-fold repercussions: loss of patients for the provider, and the patient's reluctance to pursue necessary medical care.

The Privacy Framework is designed to function as a stand-alone tool or in conjunction with any cybersecurity program, but it is also specifically designed to work with the NIST Framework for Improving Critical Infrastructure Cybersecurity, commonly known as the NIST Cybersecurity Framework (CSF).[7] HHS encourages implementation of the CSF to aid in compliance with the HIPAA Security Rule;[8] OCR released a crosswalk aligning the Security

Rule to the CSF.[9] Due to the Privacy Framework's alignment with the acclaimed CSF, and the active participation of HHS and healthcare professionals throughout development, it is highly possible that HHS and OCR will similarly embrace the Privacy Framework. There are also discussions of the OCR releasing a crosswalk aligning the HIPAA Privacy and Breach Notification Rules to the Privacy Framework.

What is the NIST Privacy Framework?

The Privacy Framework is designed to provide a catalog of privacy outcomes and approaches to identify, assess, manage, and discuss privacy risks so individuals can enjoy the benefits of evolving technologies with greater confidence and trust. The Privacy Framework is:

- Voluntary;
- Risk and outcome based, offering practices addressing the full data life cycle, including but not limited to the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of data;
- Compatible with existing domestic and international legal and regulatory regimes, in order to be the most useful to organizations and enable widespread adoption;
- Adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses;
- Scalable to organization of all sizes, public or private, in any sector, and operating within or across domestic borders;
- Agnostic as to platforms and technology; and
- Customizable in order to be useful to any organization, regardless of the existence of maturity of the organization's security and/or privacy programs.

Why NIST?

With experience in developing the widely accepted CSF, NIST is perfectly positioned to lead the creation of the Privacy Framework. For the development of the CSF, NIST collaboratively worked with the private sector and federal agencies, conducting extensive outreach through a series of workshops and requests for public comment. NIST followed the same private/federal collaboration for the Privacy Framework, which allowed tremendous input from the healthcare industry.

NIST has an extensive privacy background and has championed the critical connection between privacy and security. NIST's previous creations pertaining to privacy include:

- Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (RMF), NIST SP 800-37 released 2010, Revision 1 in 2014, and Version 2 released in 2018[10]
- An Introduction to Privacy Engineering in Risk Management, NIST IR 8062, released January 2017[11]
- Privacy Risk Assessment Methodology (PRAM) released 2017
- PRAM update released in 2019[12]

Managing privacy and security risk

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

Security Risk Model

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:

- **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

Privacy Risk Model

The Privacy Risk Model is focused on *authorized processing* of PII/PHI (planned and

permissible uses and disclosures) creating a privacy risk, resulting in loss of predictability, manageability, or disassociability, NIST's PMD Privacy Triad. PMD was introduced in NIST IR 8062.[13]

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

Problematic data actions are the issues that can result from *authorized* processing of PII/PHI. These problems may be less visible or not as well understood but result in real consequences. NIST describes them as ranging from dignity-type losses such as embarrassment, stigmas, or discrimination, to more tangible harms such as economic loss or physical harm.[14] The Privacy Framework identifies nine problematic data actions:

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

There is a clear understanding that security of data plays an important role in the protection of privacy. Cybersecurity risks arise from *unauthorized activity*. Although some privacy concerns arise from cybersecurity incidents, most privacy concerns arise from *authorized* processing of information. Figure 1 demonstrates the relationship between security concerns and privacy concerns, illustrating individual privacy cannot be achieved solely by securing data via cybersecurity controls.

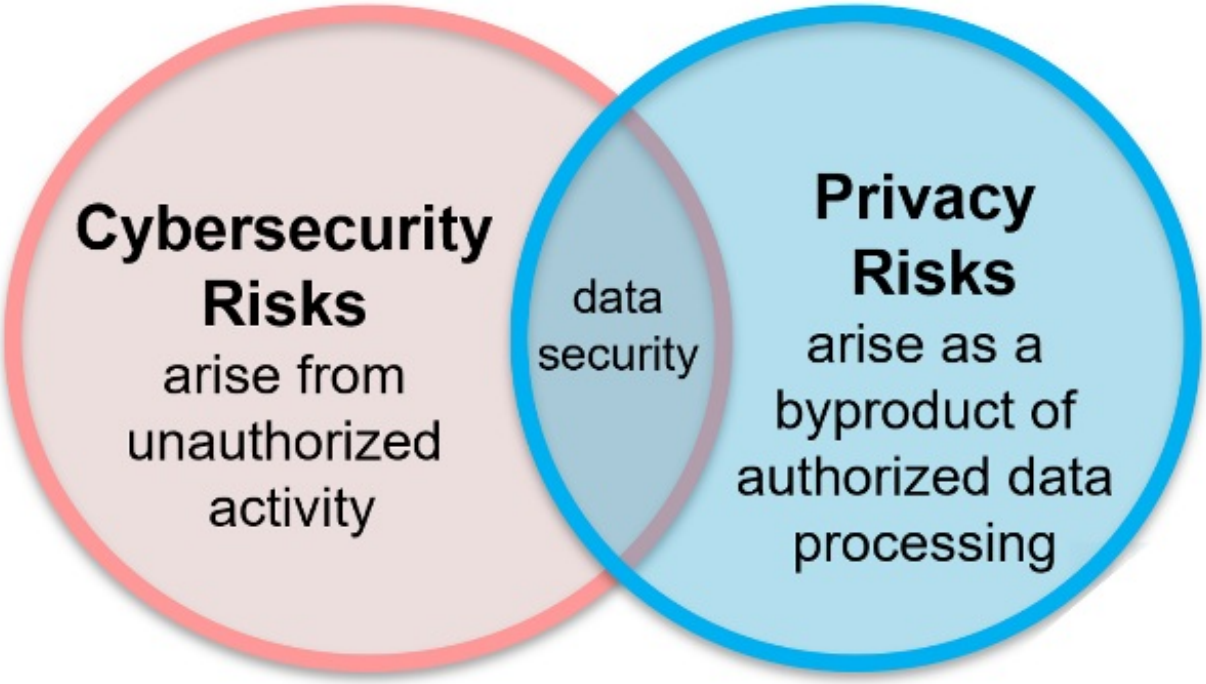

Figure 1: Cybersecurity and Privacy Risk Relationship

Recognizing the boundaries and overlap between privacy and security is key to (1) determining when existing security-focused guidance may be applied to privacy concerns, and (2) illuminating gaps that need to be filled in order 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. Given the distinctions between security and privacy concerns, entities cannot effectively manage privacy solely on the basis of managing security.

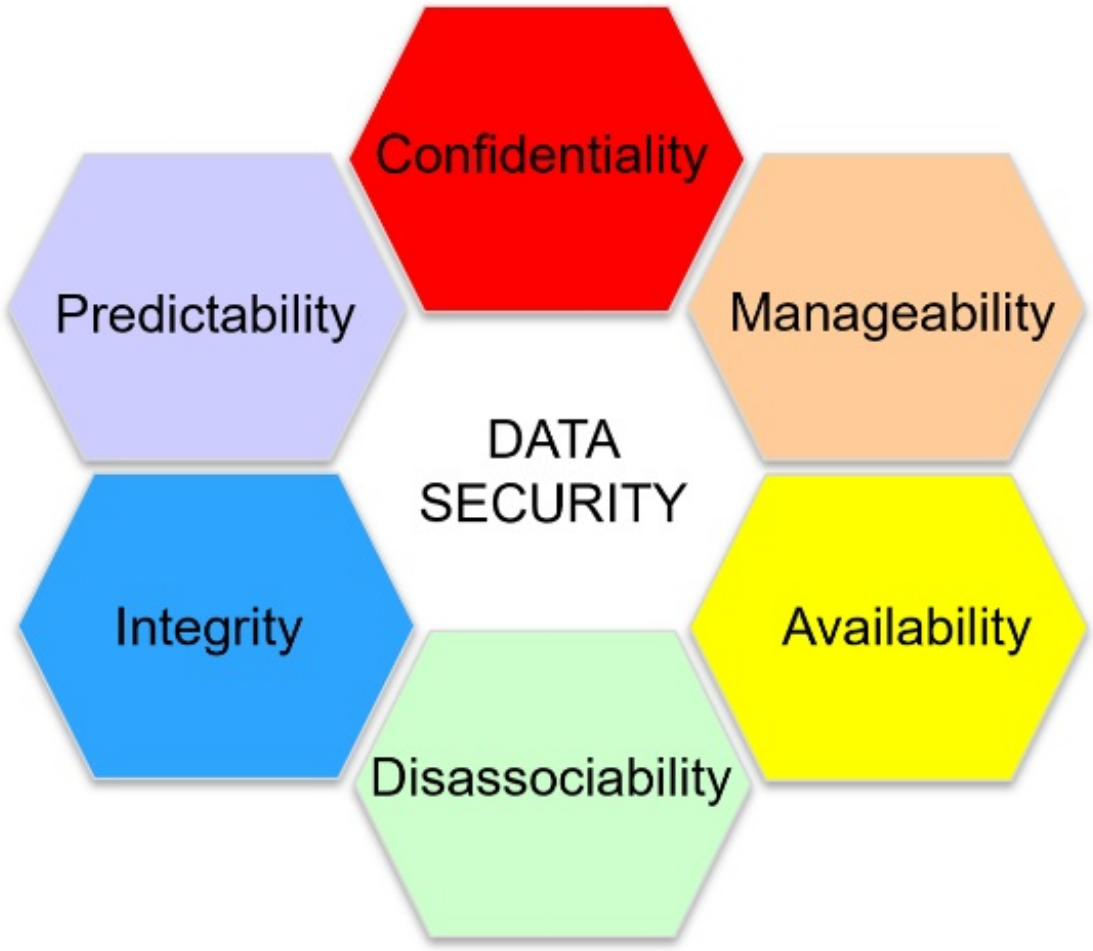

Figure 2: Full Data Security

Risk management and assessment

Privacy risk *management* is a cross-organizational set of processes that helps organizations understand how their systems, products, and services may create problems for individuals and how to develop effective solutions to manage such risks. Privacy risk *assessment* is a sub-process, producing information that can help organizations weigh the benefits of the data processing against the risks and determine the appropriate response.

The Privacy Framework is designed to enable an entity to perform a privacy risk assessment, a critical step in privacy risk management. Privacy risk assessments also help distinguish between privacy risk and compliance risk, as our NPP example illustrated. Ideally, the *privacy* risk assessment will be performed in conjunction with the entity's *security* risk assessment, giving a complete assessment of data security and allowing development of an effective enterprise risk management program (see Figure 2).

Privacy Framework overview

Designed in the familiar format of CSF, the Privacy Framework is designed in three main sections: Core, Profiles, and Tiers.

Core

The Core provides an agreed-upon set of privacy protection activities, enabling communication across the organization, and is designed to produce specific outcomes:

- **Functions** organize privacy activities at the highest level.
- **Categories** divide each Function into groups of outcomes, tied to programmatic needs and particular activities.
- **Subcategories** further divide each Category into specific outcomes of technical and/or management activities.

Profiles

The Privacy Framework calls for the creation of two profiles: current profile (the “as is” state) and target profile (the “to be” state). Development of the current profile compares the core of the Privacy Framework with the entity’s structure (e.g., business and mission requirements, risk tolerance and privacy values), current processes and resources, and current outcomes related to privacy needs of individuals. Factors considered will include the organization’s and industry sector goals, legal and regulatory requirements, industry best practices, the organization’s risk management priorities, current compliance and privacy programs, and the privacy needs of individuals.

Assessing the current profile will allow the entity to identify the ideal privacy status as a target profile. The current profile indicates which privacy outcomes an entity is currently achieving; the target profile indicates the outcomes needed to achieve the desired privacy risk management goals. Analysis of gaps between the current and target profiles forms the basis of an action plan to achieve the target profile. This allows management of privacy risk in a cost-effective, prioritized manner, by gauging the resources that would be needed (e.g., staffing, funding) to achieve the privacy outcomes identified in the target profile. Successful implementation of the Privacy Framework is based upon achieving the outcomes described in the organization’s target profile.

Implementation tiers

Tiers are intended to support enterprise privacy risk management, by considering the nature of the privacy risks and whether adequate processes and resources are in place to manage that risk. When selecting tiers, the entity will assess current management practices,

legal and business objectives, organizational privacy values, and the privacy needs of individuals.

There are four distinct tiers, each defined in the Privacy Framework according to the organization's privacy risk management processes, ecosystem relationships, and workforce training and responsibilities:

- Tier 1: Partial
- Tier 2: Risk Informed
- Tier 3: Repeatable
- Tier 4: Adaptive

Although organizations identified as Tier 1 are encouraged to work toward Tier 2, some may never need to achieve Tier 3 or 4 or may focus only on certain areas of these tiers. Although successful implementation of the Privacy Framework is based on achievement of outcomes identified in the entity's target profile, tier selection helps to set the overall tone for how privacy risk will be managed within the organization.

Using the Privacy Framework

Designed to be flexible and adaptable, the Privacy Framework offers several suggested methods for using it within organizations.

Establishing or improving a privacy program

For organizations trying to develop or improve a privacy program, the Ready–Set–Go plan offers a simple methodology. Get Ready by using the Identify function to determine the current and target profiles. Get Set by developing an action plan based on the differences between the current and target profiles. Go is implementation of the action plan. Repeat by developing the next action plan and implementing the plan.

Reviewing privacy practices

The Privacy Framework can be used to compare an organization's current privacy activities with those outlined in the Core, to examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories.

Communicating privacy risks with stakeholders

The Privacy Framework provides a common language to communicate requirements among interdependent stakeholders. Communication is especially important in supply chain risk

management (SCRM), which includes business associate agreements (BAAs) in the healthcare industry. The framework can assist in determining privacy requirements for suppliers, enacting the BAA and vendor contracts, communicating to suppliers how privacy requirements will be verified and validated, and governing the processes with business associates and venders.

Strengthening accountability

Privacy risk management can be a means of supporting accountability at all organizational levels, because it connects senior executives to those at the business/process manager level. This improves collaboration on the development and implementation of policies and procedures between management and personnel at the clinical and operational levels. Discussion and feedback between all layers of an organization are enhanced when privacy values and goals are clearly stated.

Using NIST's informative references

Subcategories can be used to identify gaps to help an entity address emerging needs, which NIST has mapped to relevant NIST guidance. Mapping subcategories to specific sections of industry standards, guidelines, and practices supports the achievement of the outcomes associated with each subcategory. The subcategories also can be used to identify where additional or revised standards, guidelines, and practices would help an organization address emerging needs. NIST has developed a process for organizations or industry sectors to submit additional informative references and mappings for publication on NIST's website.

Applying the system development life cycle

The Privacy Framework can be applied through the system development life cycle (SDLC) phases (i.e., plan, design, build/buy, operate, and decommission) by prioritizing the outcomes defined in the target profile.

The plan phase of the SDLC lays the groundwork for everything that follows, with deliberation of privacy considerations determined in the target profile. The design phase is validating that the system privacy requirements match the needs and risk tolerance of the organization as they were expressed in the target profile.

The desired privacy outcomes prioritized in a target profile should be incorporated during the build/buy phase. That same target profile serves as a list of system privacy features that should be assessed when deploying the system to verify that all features are implemented. The privacy outcomes determined by using the Privacy Framework should serve as a basis for ongoing operation of the system. This includes occasional reassessment to verify that privacy requirements are still fulfilled.

Conclusion

Application of NIST's extensive work concerning security and privacy risk management into an operational privacy framework has created a powerful tool for privacy compliance practitioners. Privacy experts understand data security and data privacy are not the same but share many objectives. Both are required for comprehensive data security. Although healthcare entities typically budget for cybersecurity, often few or no funds are designated specifically for privacy. 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 incorporate privacy security into their enterprise risk management program. Designed with collaboration between NIST and healthcare industry leaders, the Privacy Framework is a tool that may bridge the gap between security and privacy.

Takeaways

• The National Institute of Standards and Technology plans to release the new NIST Privacy Framework: An Enterprise Risk Management Tool (Privacy Framework), in October 2019.

• Representation by healthcare industry leaders in the creation of the Privacy Framework assures the framework will address the full scope of privacy.

• The Privacy Framework is structured in the familiar format of the NIST Cybersecurity Framework of core functions, current and target profiles, and implementation tiers.

• Successful implementation of the Privacy Framework is based upon achieving the outcomes described in the organization's target profile.

• Implementation tiers are intended to support enterprise privacy risk management by assessing privacy risk and evaluating processes and resources in place to manage privacy risk.

1 NIST Privacy Framework homepage. https://bit.ly/2AiwLSv
245 C.F.R. §§ 160, 162, 164 (2003) Health Insurance Reform: Security Standards; Final Rule; page 8376. https://bit.ly/2Z2k1xc
345 C.F.R. §§ 160 and 164 (2000) Standards for Privacy of Individually Identifiable Health Information; Final Rule; page 82471. https://bit.ly/2L06f4w
445 C.F.R. §§ 160 and 164, pages 82547-82552.
545 C.F.R. §§ 160 and 164 RIN 0945–AA00 (2018) Request for Information on Modifying HIPAA Rules to Improve Coordinated Care. https://bit.ly/2Bjtp0J
6 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
7 NIST *Framework for Improving Critical Infrastructure Cybersecurity* Version 1.1, April 16, 2018.

https://bit.ly/2K116rA
8 HHS.gov, HIPAA for Professionals. https://bit.ly/2JhyQmY
9 HHS.gov, HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. https://bit.ly/2zew1N2
10 NIST SP 800-37 Version 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (RMF)*, December 2018. https://bit.ly/2K3v2qU
11 Ibid, Ref #6
12NIST *Privacy Risk Assessment Methodology (PRAM)*, update released 2019, zip file download available at https://bit.ly/2KXnkvT
13 Ibid, Ref #6, Section 3.1
14 Ibid, Ref #12 "Catalog of Problematic Data Actions and Problems" zip file download available at https://bit.ly/2KXnkvT