HITRUST®

Implementing Cybersecurity in Precision Medicine

Using HPH Sector Guidance and the HITRUST CSF® to Address the PMI Data Security Policy Principles and Framework

February 2018

Contents

Preface

The intent of this paper is provide guidance and streamline the process of implementing and assuring compliance with the *Precision Medicine Initiative [PMI]: Data Security Policy [DSP] Principles and Framework*, dated 25 May 2016.

The guidance leverages the HITRUST Risk Management Framework (RMF) and existing critical infrastructure sector guidance for the implementation of the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, commonly referred to as the NIST Cybersecurity Framework (CsF), in the healthcare industry, specifically the *Healthcare Sector Cybersecurity Framework Implementation Guide*. The guide shows how healthcare and public health (HPH) organizations can fully address NIST guidance through the HITRUST RMF.

The *Precision Medicine Initiative: Data Security Policy Principles and Framework* provides requirements, but lacks the prescriptiveness and structure necessary to be effectively integrated into an organization's information privacy and security framework. This guidance along with updates to the HITRUST CSF enables organizations to easily and effectively implement and evaluate their compliance with PMI as part of their overall risk management and compliance program.

HITRUST, in its role as an industry leader in healthcare information security and privacy protection and as a public-private partner in the development of the healthcare sector-specific guide, stands ready to assist White House and federal agency efforts to develop additional guidance for PMI organizations focused on its unique sensitivities, vulnerabilities and threats.

Executive Summary

Although a relatively new field of study in the annals of medicine, precision medicine was around long before announcement of the President's Precision Medicine Initiative (PMI) in January 2015. Known by several other names, e.g., personalized or individualized medicine, precision medicine differs slightly from these earlier versions for various reasons. However, the promise of this field of study has remained the same and offers significant hope for better individual treatment and patient outcomes.

Unfortunately, great promise does not come without risk. The data used in precision medicine consists of individual genomic, demographic, environmental, lifestyle and other relevant types of personal information that is necessarily aggregated and shared extensively for both clinical and research purposes. The aggregation of so much individual personal information combined with the aggregation of multiple individual's personal information present significant additional privacy and security risk to clinical and research organizations as well as the contributors of such data.

In an effort to address the additional risks perceived with the use of data in precision medicine, there has been a concerted effort on the part of the White House, multiple federal agencies, and many industry partners to provide additional guidance on how to implement recommendations made in an earlier document, the *Precision Medicine Initiative: Privacy and Trust Principles*. These efforts focused on providing supplemental security guidance based on the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity,* commonly referred to as the NIST Cybersecurity Framework, or NIST CsF.

The *Precision Medicine Initiative: Data Security Policy Principles and Framework* provides requirements, but lacks the prescriptiveness and structure necessary to effectively integrate into an organizations information privacy and security framework. This guidance along with updates to the HITRUST CSF enable organizations to easily and effectively implement and evaluate their compliance with PMI as part of their overall risk management and compliance program.

Introduction

Originally known as personalized medicine,[1] precision medicine "refers to the tailoring of medical treatment to the individual characteristics of each patient … [by classifying] individuals into subpopulations that differ in their susceptibility to a particular disease, in the biology and/or prognosis of those diseases they may develop, or in their response to a specific treatment."[2] It is about addressing disease at the molecular level[3] while taking into consideration the "use of genomic, epigenomic, exposure, and other data to define individual patterns of disease, potentially leading to better individual treatment."[4] It is a relatively new field of medicine that holds a lot of promise, and it is one in which President Obama has taken a special interest based on his January 30, 2015 State of the Union address.

> *[Twenty-first] century businesses will rely on American science, technology, research and development. I want the country that eliminated polio and mapped the human genome to lead a new era of medicine—one that delivers the right treatment at the right time. In some patients with cystic fibrosis, this approach has reversed a disease once thought unstoppable. Tonight, I'm launching a new Precision Medicine Initiative to bring us closer to curing diseases like cancer and diabetes — and to give all of us access to the personalized information we need to keep ourselves and our families healthier.*[5]

Launched with a 2016 budget of $215 million, the President's Precision Medicine Initiative (PMI) consists of multiple efforts that span several agencies across the Department of Health and Human Services (HHS), including the National Institutes of Health (NIH), the Food and Drug Administration (FDA), and the Office of the National Coordinator for Health Information Technology (ONC). And of this $215 million, $5 million was specifically targeted for the ONC to "support the development of interoperability standards and requirements that address privacy and enable [the] secure exchange of data across systems."[6] This effort is intended to reflect the President's commitment to protecting privacy by launching "a multi-stakeholder process with HHS and other Federal agencies such as the National Institute of Standards and Technology (NIST) to solicit input from patient groups, bioethicists, privacy, and civil liberties advocates, technologists, and other experts in order to identify and address any legal and technical issues related to the privacy and security of data in the context of precision medicine."[7]

1. *"Precision medicine is a relatively new term for what has traditionally been called personalized medicine, the idea of providing health care to individuals based on specific patient characteristics." Sarata, A. and Johnson J. (2016, March 8). The Precision Medicine Initiative (IN10227). CRS Insight. Available from https://www.fas.org/sgp/crs/misc/IN10227.pdf.*
2. *National Research Council: Committee on a Framework for Developing a New Taxonomy of Disease (2011). Toward Precision Medicine: Building a Knowledge Network for Biomedical Research and Taxonomy of Disease. Wash., D.C.: The National Academies Press, p. 125.*
3. *Singal, G. (2016). Precision Medicine in the Information Age, presented at HIMSS 2016 and available from http://www.himssconference.org/sites/himssconference/files/pdf/93.pdf.*
4. *Insel, T. (2011, Nov 15). Director's Blog: Improving Diagnosis Through Precision Medicine. Available from http://www.nimh.nih.gov/about/director/2011/improving-diagnosis-through-precision-medicine.shtml.*
5. *Obama, B. (2015). State of the Union Address. Transcript available from https://pdf.yt/d/RckOjIm4grMyx9oN/download.*
6. *White House Press Office (2015, Jan 30). Fact Sheet: President Obama's Precision Medicine Initiative. Available from https://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative.*
7. *Ibid.*

In March 2015, the White House called together leading experts and interested stakeholders in both the public and private sectors to develop a set of privacy and trust principles for users of PMI data.[8] The principles, published in November 2015, provide broad guidance for "governance; transparency; participant empowerment; respect for participant preferences; data sharing, access and use; and data quality and integrity."[9] However, security is an essential component of privacy, and the White House quickly built upon the *Precision Medicine Initiative: Privacy and Trust Principles* and produced the *Precision Medicine Initiative: Data Security Policy Principles and Framework* to "guide decision making by organizations conducting or participating in precision medicine activities."[10] The security principles are consistent with the preceding privacy and trust principles, and the security framework leverages existing NIST guidance for implementing cybersecurity.

PMI Data Security Policy Principles

There are eight PMI DSP Principles, which are fully addressed by the HITRUST RMF and the *Healthcare Sector Cybersecurity Framework Implementation Guide*:

- **Strive to build a system that participants trust. This means having a "participant first" orientation when identifying and addressing data security risks.** The HPH sector guide helps ensure PMI organizations fully address the HIPAA Privacy and Security Rules' standards and implementation specifications, including the risk analysis and flexibility of approach provisions.
- **Recognize that security, medicine and technology are evolving quickly.** As a result, organizations should treat security as a core element of the organization's services and ensure that security elements are updatable. Continuous monitoring and risk management program evaluation and updates are central tenants of the HITRUST RMF and subsequently the HPH sector guide.
- **Seek to preserve data integrity, so that participants, physicians, and researchers can depend on the data.** The HPH sector guide addresses input, processing and output integrity as well as requirements for correction of records under the HIPAA Privacy Rule via implementation of the HITRUST CSF privacy practices control category.
- **Identify key risks, and develop evaluation and management plans that address those risks, while enabling science and research to advance.** The HPH sector guide provides a risk-based approach to information protection based on business needs, including clinical and research requirements.
- **Provide participants and other relevant parties with clear expectations and transparent security processes.** The HPH sector guide stresses an open and transparent assurance process for evaluating and reporting risk to internal and external stakeholders. The guidance will specifically address the ability of patients/participants to contact the organization's senior information security official and obtain information on the organizations information security practices, similar to the notification and transparency requirements outlined for privacy, with the HITRUST CSF v8 release in June 2016.

8. *White House (2015, November 9). Precision Medicine Initiative: Privacy and Trust Principles, p. 1. Available from https://www.whitehouse.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf.*
9. *Ibid.*
10. *White House (2016, February 25). Precision Medicine Initiative: Data Security Policy Principles and Framework.*

- **Use security practices and controls to protect data, but not as a reason to deny a participant access to his or her data, or as an excuse to limit appropriate research uses of the data.** The HPH sector guide provides organizations with a certain flexibility of approach when implementing its risk management program in order to accommodate appropriate uses of ePHI (electronic protected health information), including PMI data; however, the guide also requires organizations to provide a minimum expected level of due diligence and due care for the protection of patient/participant information. The guide also supports adherence to HIPAA Privacy Rule requirements around patient/participant notification, consent, and access via implementation of the HITRUST CSF privacy practices control category.
- **Act responsibly. Seek to minimize exposure of participant data, and to keep participants and researchers aware of breaches in order to maintain trust over time.** As the HPH sector guide is based on the HITRUST RMF, the guide stresses the concept of minimal necessary use and addresses both HIPAA and state-level breach notification requirements. HITRUST CSF privacy practices also require organizations to adhere to HIPAA Privacy Rule requirements around notification, consent, and acceptable use of patient/provider information.
- **Share experiences and challenges so that organizations can learn from each other.** The HPH sector guide encourages participation in external forums as well as the sharing of threat information, e.g., through the use of an Information Sharing and Analysis Organization (ISAO)[11] and participation in incident response exercises with other organizations via its proposed cybersecurity readiness maturity model. HITRUST also provides operational support through its federally-recognized ISAO, including the sharing of threat information via Cyber Threat XChange (CTX)[12] and participation in local, regional and national-level CyberRX[13] exercises.

By requiring organizations to provide a minimum level of due care and due diligence while ensuring organizations retain the flexibility of approach allowed under the HIPAA Security Rule, sector-specific guidance for implementation of the NIST CsF based on the HITRUST RMF helps ensure organizations protect the privacy of PMI participants while allowing for the most robust use of PMI data for clinical and research purposes.

11. For more information, refer to the DHS ISAO Webpage at https://www.dhs.gov/isao.

12. See the HITRUST CTX Webpage at https://hitrustalliance.net/cyber-threat-xchange for more information.

13. See the HITRUST CyberRX Webpage at https://hitrustalliance.net/cyberrx/ for more information.

PMI Data Security Policy Framework

The PMI DSP Framework is based on the NIST CsF and roughly follows its Subcategories, which provide high-level control objectives that support the framework's topical Categories and incident response-based Core Functions:[14]

- **Identify.** Develop the organizational understanding to anticipate and manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect.** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect.** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond.** Develop and implement the appropriate activities to take action regarding the detected cybersecurity event.
- **Recover.** Develop and implement the appropriate activities to maintain resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

However, while aligned with the NIST CsF Core Functions, the PMI DSP Framework does not track "1-for-1" with the NIST CsF Categories and does not specifically address each of the NIST CsF Subcategories. Subsequently, this paper will address the PMI DSP Framework more generally than the Principles.

When evaluating the PMI DSP Framework recommendations, one must also understand that (1) the HITRUST RMF and the *Healthcare Sector Cybersecurity Framework Implementation Guide* address a complete NIST CsF implementation strategy for healthcare organizations, including a comprehensive and prescriptive yet flexible set of information security controls, and (2) the PMI DSP Framework either emphasizes, enhances or adds to the control objectives provided by the NIST CsF Core. And, since the *PMI DSP Principles and Framework* were developed in parallel with the *Healthcare Sector Cybersecurity Framework Implementation Guide*, the PMI DSP Framework does not leverage the HPH sector guidance nor the HITRUST RMF. Had the efforts been coordinated, the PMI DSP Framework could have benefitted from the additional prescription provided by the HITRUST CSF controls referenced in the HPH sector guide.

The table on the following page shows how the PMI DSP Framework recommendations are addressed by the *Healthcare Sector Cybersecurity Framework Implementation Guide* through the HITRUST CSF controls. Note that the numbering schema for the Framework recommendations is derived from the structure of the *PMI DSP Principles and Framework* document and roughly follows the NIST CsF Subcategory numbering schema; however, it is not "1-to-1" with the NIST Subcategories and should not be interpreted as such. The schema in the table is simply provided as a matter of convenience.

14. NIST CsF, pp. 8-9.

PMI DSP Framework Recommendation	Supporting HITRUST CSF Controls	Number of HITRUST CSF Control Implementation Requirements Mapped but Not Modified[15]	Number of HITRUST CSF Control Implementation Requirements Mapped and Modified	Total Number of HITRUST CSF Control Implementation Requirements Mapped
ID-1. Overall Security Plan	03.a, 04.a, 04.b, 05.a	8	3	11
ID-2. Risk-based Approach	03.a, 07.d	8	1	9
ID-3. Independent 3rd-Party Review	05.a, 05.h	1	1	2
ID-4. Transparency	05.j	0	1	1
PR.AC-1. Identify Proofing	01.q, 02.b, 02.d, 05.j, 13.j	3	3	6
PR.AC-2. Credentials	01.q	0	2	2
PR.AC-3. Authentication	01.q	0	1	1
PR.AC-4. Authorization	01.b	0	1	1
PR.AT-1. Participant Education	05.j	0	1	1
PR.AT-2. PMI Data User Education	02.e	2	0	2
PR.DS-1. Encryption	01.n, 01.x, 06.c, 06.d, 09.m, 09.o, 09.s, 13.l	9	0	9
PR.DS-2. Encryption Key Security	06.c, 06.d, 10.g	4	1	5
PR.DS-3. Physical Security	08.d	1	0	1
PR.DS-4. Service Provider Integrity	05.i	1	0	1
PR.DS-5. Integrity Protection	09.aa, 09.ab, 10.b, 10.c, 10.d	9	0	9
PR.IP-1. Lifecycle	10.a	1	0	1
PR.IP-2. Security Patching	01.y, 10.k, 10.m	5	0	5
DE-1. Audit Events	06.i, 09.aa	10	0	10
DE-2. Audit Logs	09.aa, 09.ab, 09.ac	6	0	6
DE-3. Detection and Alerting	09.ab	3	0	3
DE-4. Threat Information Sharing	05.g, 11.a, 11.b	9	0	9
DE-5. Anomaly Reporting	05.a, 11.c	2	0	2
RS-1. Incident Response	03.b, 05.e, 05.f, 05.j, 05.k, 11.a, 11.c	15	0	15
RS-2. Incident Response Testing	11.c	2	0	2
RS-3. Affected Individual Notification	11.a	4	0	4
RS-4. Accountable Point of Content	11.c	0	1	1
RC-1. Incident and Breach Recovery Plan	09.l, 11.c, 12.c	12	0	12
RC-2. Communication	11.c	0	1	1
RC-3. Lessons Learned	05.b, 11.c, 12.e	5	0	5
Total	**50 (Unique)**	**120**	**17**	**137**

Table 1. Mapping of HITRUST CSF Controls/Requirements to the PMI DSP Framework

15. A HITRUST CSF control contains multiple implementation specifications distributed amongst up to three levels, the selection of which is based on an organization's specific organizational, system and regulatory risk factors.For more information, see Cline, B. (2016, Feb). Risk Analysis Guide for HITRUST Organizations and Assessors: A guide for self- and third party assessors on the application of HITRUST's approach to risk analysis. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf.

For a more complete description of how the PMI DSP framework recommendations are addressed in the HITRUST CSF, refer to the 2016 release of the *HITRUST CSF v8 Summary of Changes*.[16]

A comparison of the PMI DSP Framework with the HITRUST CSF shows that the PMI DSP Framework addressed 50 of the CSF's 146 security and privacy controls, and only 47 of 135 security controls. The HITRUST CSF has more than 2,000 comprehensive implementation requirements, and the PMI DSP Framework mapped directly to less than 7% and impacted less than 1%.

There were also no substantially new requirements generated as a result of the crosswalk, with the possible exception of allowing an individual to contact the organization's senior security official and receive information about the security program. In general, the 17 modifications that were made to the HITRUST CSF either clarified or enhanced a pre-existing implementation requirement.

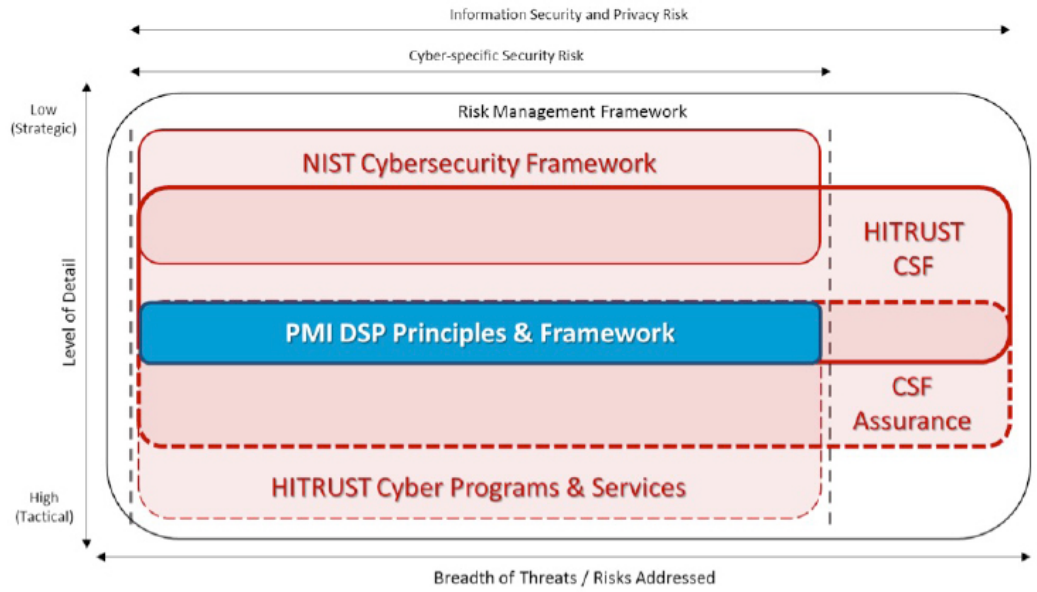
For example,[17] PMI DSP Framework ID-2 modified an existing implementation requirement in HITRUST control 07.d to consider aggregation when classifying data and specifying associated protective controls to other forms of data, such as raw data and data that is the product of a mathematical or statistical process or analysis report. Another modification was made to HITRUST CSF control 01.q to require contributors of PMI data to be uniquely identified in addition to those individuals accessing the organization's PMI data.

One should also note that the HITRUST CSF generally specifies numerous other control requirements that provide additional prescription for the NIST CsF Subcategories upon which the PMI DSP Framework is based, and the selection of these controls is dependent on specific organizational, system and regulatory risk factors.[18] This approach allows healthcare organizations to tailor the HITRUST CSF controls to their unique clinical and business risk environment consistent with NIST guidance on tailoring[19] and the creation of overlays,[20] and generally supports the HIPAA Security Rule's provisions for flexibility of approach[21] in the specification of a reasonable and appropriate set of administrative, technical and physical safeguards necessary to adequately protect patient/participant information.

Although it's clear from the *Healthcare Sector Cybersecurity Framework Implementation Guide* that the HITRUST RMF provides a model implementation of the NIST CsF for the industry, including by definition PMI organizations, there are still misconceptions by some about the relationship of the NIST CsF, the *Healthcare Sector Cybersecurity Framework Implementation Guide*, and the *PMI DSP Principles and Framework*.

16. *The HITRUST CSF v8 Summary of Changes is part of the HITRUST CSF v8 download package available through the HITRUST CSF License Agreement Webpage at https://hitrustalliance.net/csf-license-agreement/.*
17. *The specific changes made to the HITRUST CSF to address the PMI DSP Framework recommendations are available in the HITRUST CSF v8 Summary of Changes*
18. *Cline, B. and Frederick, M. (2016). HITRUST CSF Risk Factors: How HITRUST uses risk factors to help healthcare organizations dynamically tailor CSF controls to meet their information protection needs, including changes for the 2016 CSF v8 release. Frisco, TX: HITRUST.Available from https://hitrustalliance.net/documents/csf_rmf_related/v8/CSFRiskFactorsGuide.pdf.*
19. *NIST (2013). Security and Privacy Controls for Federal Information Systems (NIST SP 800-53 rev 4), pp 30-40. Gaithersburg, MD: Author. Available from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*
20. *Ibid., pp. 40-41.*
21. *See 45 CFR 164.306(b).*

For example, there has been a call by some to expand upon the PMI guidance and provide additional prescription around basic information security practices that support the objectives specified by the NIST CsF Subcategories. One such example is a request for clarification around the role of the cyber incident response team in relation to the overall organizational incident response and data breach notification process. Another is a recommendation that an overall security plan should be written and reviewed and updated regularly. These and many other issues like this, in which additional prescription is requested to address the objectives specified by the NIST CsF Subcategories, have already been addressed in the *Healthcare Sector Cybersecurity Framework Implementation Guide* through the HITRUST RMF and its major components: the HITRUST CSF and CSF Assurance Program, as illustrated in the following figure.



The NIST CsF is an overarching, high-level, industry-agnostic framework that guides development of a cybersecurity program. As such, it is specific to cyber-related security risks and provides strategic-level control objectives, i.e., it's guidance has a relatively low level of detail. The HITRUST CSF incorporates much of the guidance contained in the NIST CsF and then adds a significant amount of prescriptive controls tailored to the healthcare sector that support the strategic-level objectives of the NIST CsF Core. The HITRUST CSF also provides slightly greater breadth than the NIST CsF in that it incorporates non-cyber-related security as well as privacy directly into the control framework. The HITRUST CSF Assurance Program provides additional granularity through its illustrative procedures and control maturity and scoring models. HITRUST cyber programs and services provide even more detail due to their operational nature, e.g., the actual exchange of threat information and conduct of incident response exercises. And as shown previously, the HITRUST CSF v8 release fully incorporates the guidance provided in the *PMI DSP Principles & Framework*.

Rather than "reinventing the wheel" and asking for new healthcare sector-specific guidance for implementation of the NIST CsF, the PMI community and interested stakeholders in the protection of PMI data should instead ask two very specific questions:

1. How is PMI data different from other types of PII/PHI in terms of sensitivity and the subsequent protections required? For example, PMI data is generally aggregated, which is a form of data that must be considered when developing its classification and relevant protections.
2. How is PMI data used differently in terms of clinical and research work flows that present risks that are unique to PMI data? For example, the collection of standardized molecular, exposure, and clinical data useful for research as part of routine health care[22] would help facilitate PMI research; however, the collection and aggregation of such information at the clinical level could potentially present more risk to patient/participant information and the PMI organization.

In this way, additional guidance on implementation of the NIST CsF by PMI organizations will focus on a very special subset of recommendations that address threats and vulnerabilities that are truly unique to PMI data.

Conclusion

Precision medicine is one of the most promising fields of medicine in the 21st century, which is arguably the reason for President Obama's 2015 announcement of his Precision Medicine Initiative. But with this promise comes increased concern about the security and privacy of PMI data, a relatively special use case for PII/PHI. Fortunately, the general security concerns of PII/PHI and similar types of covered information have been addressed by the Joint HPH Cybersecurity WG in its 2016 publication of the *Healthcare Sector Cybersecurity Framework Implementation Guide*. This sector-specific guidance for implementation of the NIST CsF by healthcare organizations is based extensively on the HITRUST RMF, which provides the most comprehensive, risk-based information protection control framework in the healthcare industry as well as a robust internal and external (third party) assurance program that helps organizations streamline their third party assessment processes and associated costs. The HITRUST CSF v8 release available in early summer 2016 fully addresses the recommendations of the President's *PMI DSP Principles and Framework*, published in May 2016 and is intended to provide a basis for PMI organizations for their own information protection programs.

However, the PMI guidance does not, by itself, provide the level of prescription necessary for implementation of the NIST CsF nor does it leverage the prescription available in the joint working group's sector-specific guide.

22. From Insel (2011, November 15). Available from http://www.nimh.nih.gov/about/director/2011/improving-diagnosis-through-precision-medicine.shtml.

Subsequently, additional work on addressing NIST CsF implementation for PMI organizations should focus on specific administrative, technical and physical safeguards that address specific sensitivities, vulnerabilities and threats that are unique to PMI data as compared to traditional uses cases for PHI. HITRUST, as an industry leader in health information protection and as a public partner for the White House and multiple federal agencies addressing privacy and security issues, stands ready to assist extant and emerging PMI community efforts in (1) properly defining the work needed and (2) developing PMI-specific guidance that focuses on the unique characteristics of PMI data. Such guidance should then be integrated with other data and organization-specific guidance, e.g., medical device security and small, low-risk organization implementation, which are currently under development by the HITRUST community.

About HITRUST

Founded in 2007, the Health Information Trust Alliance (HITRUST) was born out of the belief that information protection should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST—in collaboration with public and private healthcare technology, privacy and information security leaders—has championed programs instrumental in safeguarding health information systems and exchanges while ensuring consumer confidence in their use.

HITRUST programs include the establishment of a common risk and compliance management framework (CSF); an assessment and assurance methodology; educational and career development; advocacy and awareness; and a federally recognized cyber Information Sharing and Analysis Organization (ISAO) and supporting initiatives. Over 84 percent of hospitals and health plans, as well as many other healthcare organizations and business associates, use the CSF, making it the most widely adopted security framework in the industry. All this is part of the HITRUST commitment to help healthcare organizations manage many diverse requirements with one comprehensive framework.

For more information, visit *www.HITRUSTalliance.net*.

Appendix: Supplemental Material

NIST Guidance

The NIST *Framework for Improving Critical Infrastructure Cybersecurity*,[23] commonly referred to as the Cybersecurity Framework (CsF), was developed as the result of President Obama's Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*.[24] The NIST CsF provides an overarching incident management-based approach to cybersecurity that is intended to apply broadly across all organizations, regardless of size, industry, or cybersecurity sophistication. Whether an organization has a mature risk management program and supporting processes, is developing a program or process, or has no program or process, the NIST CsF can help guide an organization in improving cybersecurity and thereby improve the security and resilience of critical infrastructure.

But because the NIST CsF is a high-level framework, there are many ways in which it may be implemented by a sector, sub-sector or even individual organizations to suit their particular needs. Therefore, some sectors such as critical manufacturing and emergency services have produced additional guidance[25] to help facilitate the NIST CsF's implementation at the organizational level, and the healthcare and public health (HPH) sector is no exception.

HPH Sector Guidance

In addition to creation of the NIST CsF, E.O. 13636 called on Sector-specific Agencies like HHS to "coordinate with the Sector Coordinating Councils[26] [SCC] to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments." The Joint HPH [Government Coordinating Council[27] (GCC) and SCC] Cybersecurity Working Group (WG)—created under Presidential Policy Directive (PPD) 21,[28] *Critical Infrastructure and Security and Resilience*—subsequently launched a Risk Management (RM) Sub-working Group (SG) in 2015 to build upon the work of existing organizations within the HPH Sector to advance the implementation of the NITS CsF in the Sector and provide a forum for discussion of cybersecurity issues related to risk management among a wide variety of HPH Sector stakeholders.

23. *Available directly from NIST at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.*
24. *The Executive Order is available from the White House Website at https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.*
25. *Some of these guidance documents are available from the US-CERT Website at https://www.us-cert.gov/ccubedvp/cybersecurity-framework.*
26. *More information on Sector Coordinating Councils can be found on the DHS Website at https://www.dhs.gov/scc.*
27. *More information on Government Coordinating Councils can also be found on the DHS Website at https://www.dhs.gov/gcc.*
28. *PPD-21 is available from the White House Website at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.*

Co-chaired by the Health Information Trust Alliance (HITRUST)[29] and HHS/ONC and supported by multiple organizations across the HPH sector, the RM SG completed its initial draft of healthcare-specific implementation guidance in December 2015, which was later reviewed and approved for release by the Joint HPH Cybersecurity WG in April of 2016. A revised 508-compliant[30] version of the *Healthcare Sector Cybersecurity Framework Implementation Guide* ("HPH sector guide") was developed and released two months later, and is now available from both HITRUST[31] and DHS.[32]

The HPH sector guide presents background information on the NIST CsF and HITRUST Risk Management Framework (RMF),[33,34]including potential benefits to HPH sector organizations; explains the relationship between the two frameworks and how the HITRUST RMF provides a model implementation of the NIST CsF for the Healthcare Sector; presents a mapping of HITRUST CSF controls to the NIST CsF subcategories; and integrates the Office of Civil Rights (OCR) crosswalk between the Health Insurance Portability and Accountability Act[35] (HIPAA) Security Rule and the NIST CsF.[36]

The HPH sector guide helps HPH sector organizations understand and use the HITRUST RMF as healthcare's implementation of the NIST CsF, supports implementation of a sound cybersecurity program that addresses the five Core Function areas of the NIST CsF to ensure alignment with national standards, helps organizations assess and improve their level of cyber resiliency, and provides suggestions on how to link cybersecurity with their overall information security and privacy risk management activities to the Healthcare Sector.

The HPH sector guide is also intended to help an organization's leadership:

- Understand NIST CsF and HITRUST RMF terminology, concepts, and benefits
- Assess their current and targeted cybersecurity posture
- Identify gaps in their current programs and workforce
- Identify current practices that exceed NIST CsF requirements

29. *See the HITRUST Website for more information on the HPH sector alliance: https://hitrustalliance.net.*
30. *"Section 508, an amendment to the United States Workforce Rehabilitation Act of 1973, is a federal law mandating that all electronic and information technology developed, procured, maintained, or used by the federal government be accessible to people with disabilities." (http://searchcio.techtarget.com/definition/Section-508)*
31. *Available directly from the HITRUST Website at https://hitrustalliance.net/documents/cybersecurity/HPHCyberImplementationGuide.pdf.*
32. *Available via a link from the DHS US-CERT Website at https://www.us-cert.gov/ccubedvp/cybersecurity-framework.*
33. *The HITRUST RMF—consisting of the CSF, CSF Assurance Program, and supporting methods, tools and services—is a model implementation of the NIST CsF. Consistent with the NIST framework, the HITRUST CSF provides a comprehensive, prescriptive, yet flexible, information security control framework that leverages the risk analyses used to develop its supporting authoritative sources. The CSF Assurance Program complements the CSF by providing the mechanism for sharing information security assurances with internal and external stakeholders in a consistent and repeatable way.*
34. *A joint presentation by Health Care Services Corporation (HCSC) and Children's Health on a healthcare organization's rationale for selecting the HITRUST RMF over other frameworks is available from the HITRUST Website at https://hitrustalliance.net/content/uploads/2016/01/HCSC_Childrens_Health_Selecting_Healthcare_Information_Security_RMF_in_a_Cyber_World.pdf.*
35. *The HIPAA Administrative Simplification Regulation Text is available from HHS at http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.*
36. *A copy of the OCR crosswalk between HIPAA and the NIST CsF can be downloaded from the HHS Website at http://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/.*

PMI Guidance

As mentioned earlier, the *PMI Data Security Policy [DSP] Principles and Framework*[37] was originally published in February 2016. But the White House quickly followed up with a second version on May 25, 2016 to clarify there are a number of frameworks—besides the NIST CsF—that PMI organizations could potentially use to help address their cybersecurity requirements. It also recommends they "select the security framework that adequately addresses the security risks they face and is consistent with the *PMI Data Security Policy Principles and Framework*."[38]

But while the White House recognized in its announcement of the 'final' version that "organizations can use the [PMI security] framework to develop detailed implementation guidelines that address their specific data security needs" and that "[ONC, OCR], in partnership with NIST, other Federal Partners, and a broad set of stakeholders, will release a [PM]-specific guide to the NIST [CsF] by December 2016],[39] "the fact the NIST CsF is an overarching, high-level framework that can help guide the specification[40] and implementation of an organization's information protection program is not made clear within the PMI guidance itself.

As an overarching framework for cybersecurity implementation across multiple sectors, the NIST CsF:

- Provides guidance on risk management principles and best practices,
- Provides a common language to address and manage cybersecurity risk,
- Outlines a structure for organizations to understand and apply cybersecurity risk management, and
- Identifies effective standards, guidelines, and practices to manage cybersecurity risk in a cost-effective manner based on business needs.

The approach taken in the *Healthcare Sector Cybersecurity Framework Implementation Guide* is similar, as it shows how an underlying framework like the HITRUST RMF can be used to satisfy one of the principle goals of the NIST CsF, which is to improve cybersecurity and thereby improve the security and resilience of critical infrastructure.

37. *The PMI DSP Principles and Framework is available from the White House Website at https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/PMI_Security_Principles_Framework_v2.pdf*
38. *Ibid., p. 4*
39. *The White House. (2015, May 25). Precision Medicine Initiative and Data Security. Available from https://www.whitehouse.gov/blog/2016/05/25/precision-medicine-initiative-and-data-security.*
40. *This specification can be based on a traditional risk analysis or, as demonstrated in the NIST CsF's informative references, specification can leverage a more comprehensive and prescriptive information protection framework,such as that provided by the Organization for International Standardization (ISO) 27000-series publications, NIST 800-series special publications, or HITRUST RMF documentation.*

The PMI guidance also recognizes that many of the principles it outlines may already be required of certain PMI organizations by other applicable laws and states, "PMI organizations will comply with all applicable laws and regulations governing privacy, security, and the protection of PMI data at every stage of data collection, storage, analysis, maintenance, use, disclosure, exchange, and dissemination."[41] This is consistent with the position that PMI is essentially a subset of protected health information (PHI)[42] and a PMI organization must necessarily comply with the HIPAA Privacy and Security Rules if they are a covered entity or a business associate.[43] There may also be other regulations or standards for which a PMI organization must comply. For example, individual records held by covered entities that are also alcohol and substance abuse treatment providers are protected by the Federal Confidentiality of Alcohol and Substance Abuse Patient Records Regulation (see 42 CFR part 2), and the HHS and the U.S. Food and Drug Administration (FDA) Protection of Human Subjects Regulations (45 CFR part 46 and 21 CFR parts 50 and 56, respectively) may apply to health services research.[44]

This further demonstrates that a comprehensive and harmonized information protection framework like the HITRUST CSF—an essential part of the HITRUST RMF and the basis of current sector-specific guidance for NIST CsF implementation—can be used to satisfy another goal of the NIST CsF: to help organizations manage cybersecurity risk in a cost-effective manner based on business needs, which includes regulatory compliance.

41. Ibid., p. 1

42. The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI). See http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/.

43. See the NIH position on clinical research and the HIPAA Privacy Rule at https://privacyruleandresearch.nih.gov/clin_research.asp.

44. Ibid.

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net