Journal of Diabetes Science and Technology
2017, Vol. 11(2) 220–223

DOI: 10.1177/1932296816680006
journals.sagepub.com/home/dst
SAGE

The Need for a Privacy Standard for Medical Devices That Transmit Protected Health Information Used in the Precision Medicine Initiative for Diabetes and Other Diseases

David C. Klonoff, MD, FACP, FRCP (Edin), Fellow AIMBE[1] and W. Nicholson Price II, PhD, PD[2]

Abstract

Privacy is an important concern for the Precision Medicine Initiative (PMI) because success of this initiative will require the public to be willing to participate by contributing large amounts of genetic/genomic information and sensor data. This sensitive personal information is intended to be used only for specified research purposes. Public willingness to participate will depend on the public's level of trust that their information will be protected and kept private. Medical devices may constantly provide information. Therefore, assuring privacy for device-generated information may be essential for broad participation in the PMI. Privacy standards for devices should be an important early step in the development of the PMI.

Keywords

HIPAA, precision medicine, privacy, protected health information, security, standard, diabetes

The Precision Medicine Initiative (PMI) is intended to promote developments in precision medicine. Precision medicine is a recently recognized paradigm for combining new types of metrics with big data sets. This paradigm can be applied to diabetes and other diseases.[1] Precision medicine creates predictions for prevention, diagnosis, and specific therapies from advances in sensors, software analytics, genetics, and systems biology. The expanding use of wearable sensors for digital phenotypic assessment and behavioral monitoring is providing a great deal of information that can become part of a precision medicine paradigm. Privacy is an important concern for the PMI because success of this initiative will require the public to be willing to participate by contributing large amounts of genetic/genomic information and sensor data that will be analyzed for risk factors for various diseases. This personal information will be very sensitive and is intended to be used for only specified research purposes. Public willingness to participate will depend on the public's level of trust that their information will be protected and kept private.

In November 2015 the National Institutes of Health (NIH) announced a set of privacy and trust principles for the PMI to ensure the confidentiality and integrity of all PMI cohort data and specimens.[2] These principles are aimed at protecting patient privacy for PMI-related activities and building trust. They consist of six values, including:

1. **Governance**, including mandatory rules and mechanisms to ensure accountability; responsible data management; protection against unauthorized access, use, disclosure, or reidentification of PMI data; and proper identification, management, and mitigation of breaches.
2. **Transparency**, including clear information to participants about how information will be collected and stored; how data will be used and shared; what goals, potential benefits, and risks of participation will be; the measures that will protect participant data; and the mechanism to withdraw participation.
3. **Respect** for participant preferences through subject control of how PMI is shared and how participants should be able to withdraw consent for future use and sharing of PMI data at any time.

[1]Diabetes Research Institute; Mills-Peninsula Health Services, San Mateo, CA, USA
[2]University of Michigan Law School, Ann Arbor, MI, USA

Corresponding Author:
David C. Klonoff, MD, FACP, FRCP (Edin), Fellow AIMBE, Diabetes Research Institute, Mills-Peninsula Health Services, 100 S San Mateo Dr, San Mateo, CA 94401, USA.
Email: dklonoff@diabetestechnology.org

4. **Empowerment** of participants through access to information that a subject has provided.
5. **Privacy** by restricting access to and use of PMI data to authorized purposes; by prohibiting use of this data for targeted advertising, unauthorized reidentification, and unauthorized recontacting of PMI participant; and by mandating tiered access based on the type of data, purpose of access, and qualifications of users.
6. **Data quality and integrity** thorough a mechanism allowing subjects to report inaccuracies and for the inaccuracies to be repaired.

In the United States, there is no widely recognized standard for privacy of information that will be used in big data sets for precision medicine. The most important federal law governing health information in the United States is the Health Insurance Portability and Accountability Act (HIPAA). This law applies to specifically designated "covered entities," which include health care providers, health plans, and health information clearinghouses; their business associates are also required to abide by HIPAA's rules.

HIPAA has three purposes relating to medical information, including: (1) to establish structures both for how protected health information (PHI) may be disclosed; (2) to create security standards for patient information at rest and in motion; and (3) to specify a common format and data structure for electronic exchange of health information. PHI is any individually identifiable health information created or collected by a covered entity or business associate.[3]

The part of HIPAA covering information privacy is called the Privacy Rule, which regulates how health information may be disclosed, both with and without a patient's consent. This rule authorizes disclosures of PHI without patient consent for treatment, payment, and routine health care operations. In addition, no consent is necessary for such disclosures of information as mandatory reporting to public health agencies, informing law enforcement or national security, and determining eligibility for public benefits.[4] HIPAA's Privacy Rule recognizes that identifiable health information is especially sensitive for many patients, and tries to limit the objective, subjective, and dignitary harms that may result from the disclosure of that information.

In 2015, President Obama announced that the White House is seeking $130 million for NIH to develop a national cohort of at least one million volunteers for a longitudinal study, plus an additional $85 million for additional supporting projects for this initiative. Their medical, physiological, and genomic data would be integrated in a massive database that would be made available to researchers. This database will incorporate data from medical records, research study records, biospecimens, claims data, and mobile devices to correlate various health measures and environmental exposures with each participant's outcomes.[5]

An important feature of this project will be recontactability, which means permission from biobank patients to be called and asked to come to a clinic for reconsenting followed by further exams and tests. This is especially important because one approach researchers often use to comply with HIPAA is to deidentify data; once data are no longer individually identifiable, they are not covered by the HIPAA Privacy Rule.[6]

For the PMI, privacy and security are linked issues. Statistical analysis methods can be used to link phenotypes to genotypes using publicly available genotype-phenotype correlations. Entries in genotype and phenotype data sets when linked can reveal sensitive information.[7] Protecting the privacy of participating individuals will be an important issue in the genotype-phenotype association studies that will be central to the PMI.[8] Privacy of a patient's identity could be maintained by applying various remedies to a genomic data set (data at rest) located on a server, including: (1) to combine data sets to expand the size of the database and obscure where the individual patient's data was residing (although big data sets tend to be big targets for hackers and are not necessarily protected from hacking); (2) restricting access to trusted database users; and (3) establishing tiers of secured access and then requiring users to be authorized for data access.

Privacy must be addressed in any major health care data warehousing project, such as the PMI. If the PMI does not provide clear privacy protections for its activities, then individuals will probably be reluctant to volunteer to submit their data. On May 16, 2016, the World Privacy Forum published a report finding that the PMI has failed to address many core privacy questions.[9]

They raised five types of concerns about privacy protections of medical data and biospecimen data donated to this initiative:

1. Medical record data and biospecimen data donated to the PMI are not covered by the core federal health privacy law, HIPAA, while in the hands of the PMI because the NIH, which is spearheading the initiative, is not considered one of the three types of HIPAA-covered entities: health care providers, payers, and health care clearinghouses.
2. Patients who share their health records and biospecimens with the PMI could lose the ability to claim a physician-patient privilege in unrelated judicial proceedings.
3. The possibility of law enforcement access to patient records held in the PMI has not been addressed by the PMI, nor have donors been informed of how law enforcement access to the data will be handled.
4. Consumers may have no formal legal right to obtain their own information from the PMI unless a US government agency administers the PMI, something that is not expected.

5. A process for handling real time monitoring data that is not derived from medical records or biospecimens (such as from glucose monitors, continuous glucose monitors, insulin pens, insulin pumps, artificial pancreas systems, cell phones, social media, physiological sensors, and global positioning systems) has not been determined.

This nonprofit public interest research and consumer education group focusing on privacy-related issues recommended that the PMI clarify the legal and administrative privacy protections that apply to its activities before it begins to begin solicit information or biospecimens. They concluded that to maximize participation by individuals, who will be volunteering to submit their data and biospecimens, these people must be informed about which legal protections apply.

In May 2016 the White House released a set of data security principles and a framework for the PMI, intended to protect patient data and resources in an appropriate and ethical manner.[10] The document was developed with input from multiple government agencies and discussions with security experts (including one of the authors of this article: DCK). The developers of this framework recognized that patient-contributed data are the foundational asset of the PMI and participants deserve assurance that the data are being protected and used responsibly. The framework was intended to establish trust and encourage widespread participation and donation of health data. The document established a set of eight data security policy principles for PMI organizations (Table 1). The document then recommended use of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, released in 2014, which defines a set of five types of activities to assess cybersecurity and data security performance, as well as physical and environmental controls. The five recommended activities for data security programs are listed in Table 2.

Table 1. Eight Data Security Policy Principles for PMI Organizations Specified in the Precision Medicine Initiative Data Security Policy Principles and Framework.

1) Strive to build a system that participants trust. This means having a "participant first" orientation when identifying and addressing data security risks. Participants are the foundational stakeholders of all research activities.
2) Recognize that security, medicine, and technology are evolving quickly. As a result, organizations should treat security as a core element of the organization's culture and services and ensure that security processes and controls are adaptable and updatable.
3) Seek to preserve data integrity, so that participants, researchers, and physicians and other health care providers, can depend on the data.
4) Identify key risks, and develop evaluation and management plans that address those risks, while still enabling science and research to advance.
5) Provide participants and other relevant parties with clear expectations and transparent security processes.
6) 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.
7) 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.
8) Share experiences and challenges so that organizations can learn from each other.

Table 2. Five Recommended Activities According to the NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0.

1) Identify
2) Protect
3) Detect
4) Respond
5) Recover

On September 15, 2016, NIH Director Francis Collins commented on the privacy challenges surrounding the PMI from a perspective that privacy is a priority.[11] He stated that "people are being asked to make available their electronic health records and there's a lot of personal, private information in it, with the expectation that that's going to be a trusted donation that will be handled with great care and will not be falling into the hands of bad people." He also stated that "we will not actually launch this until we're confident on a variety of tests, so-called penetration tests, that we have the toughest possible firewall against mischief." We concur with this caution in not launching the PMI until its privacy protection systems are firmly established.

Given the need to protect the privacy of data from devices we recommend that the stewards of PMI data should support development of privacy standards for devices that collect and transmit PHI. In this way information donors to the PMI could be reassured that the types of vulnerability assessments and penetration tests that the US government might perform on devices that will transmit data from sensors to a central data repository (data in motion) will be appropriate and adequate. There have been many highly publicized security breaches of companies, hospitals, and government agencies.[12-14] Prospective donors of personalized data to the PMI might not trust the data repositories to preserve privacy, even if NIH will develop and then claim to adhere to performance of future privacy performance standards are. Assurance by disinterested qualified third-party test labs is needed to confirm that privacy standards are adequately being adhered to.[15] Security through meeting both performance requirements as well as assurance requirements are the basis of Common Criteria, also known as ISO 15048, a software security standard. These two types of requirements are the basis of DTSec, the Diabetes Technology Society

Cybersecurity Standard for Connected Diabetes Devices, which is the first broad based consensus standard with FDA participation.[16] This standard can be used as a template for creating a privacy standard for devices that transmit information wirelessly for the PMI. Adherence to such a standard will provide PMI device stakeholders (eg, patients, health care professionals, researchers, and the government) with more than mere claims of information security by manufacturers; instead, they can rely on information security assured by a rigorous testing process.

Security standards are important to ensure privacy but are not enough. Privacy standards should also ensure that even those permitted access to the data do not misuse them, such as by selling or distributing the data or using them for commercial purposes like marketing. Privacy is a key value for patient participation in the PMI; privacy standards can help facilitate patient trust and participation.

Abbreviations

DTSec, Diabetes Technology Society Cybersecurity Standard for Connected Diabetes Devices; HIPAA, Health Insurance Portability and Accountability Act; NIH, National Institutes of Health; NIST, National Institute of Standards and Technology; PHI, protected health information; PMI, Precision Medicine Initiative.

Acknowledgments

The authors thank Annamarie Sucher for her expert editorial assistance.

Declaration of Conflicting Interests

The author(s) declared the following potential conflicts of interest with respect to the research, authorship, and/or publication of this article: DCK is a consultant for Insulet, LifeCare, and Voluntis. WNP has no disclosures.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

1. Klonoff DC. Precision medicine for managing diabetes. *J Diabetes Sci Technol*. 2015;9(1):3-7.
2. Handelsman JO, Patil DJ. Building trust and protecting privacy: progress on the President's Precision Medicine Initiative. November 9, 2015. Available at: https://www.whitehouse.gov/blog/2015/11/09/releasing-privacy-and-trust-principles-precision-medicine-initiative. Accessed October 26, 2016.
3. 45 CRF § 160.103.
4. 45 CRF §§ 164.502-512.
5. White House, Office of the Press Secretary. Fact Sheet: President Obama's Precision Medicine Initiative. January 30, 2015. Available at: https://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative. Accessed October 26, 2016.
6. 45 CRF § 164.514(a).
7. Ohm P. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Rev*. 2010;57:1701.
8. Harmanci A, Gerstein M. Quantification of private information leakage from phenotype-genotype data: linking attacks. *Nat Methods*. 2016;13(3):251-256.
9. Gellman R, Dixon P. The Precision Medicine Initiative and privacy: will any legal protections apply? May 18, 2016. Available at: http://www.worldprivacyforum.org/wp-content/uploads/2016/05/WPF_PrecisionMedicineInitiative_May2016_fs.pdf. Accessed October 26, 2016.
10. White House. Precision Medicine Initiative: data security policy principles and framework. May 25, 2016. Available at: https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/PMI_Security_Principles_Framework_v2.pdf. Accessed October 26, 2016.
11. Bowman D. Francis Collins: privacy a priority for Precision Medicine Initiative. September 15, 2016. Available at: http://www.fiercehealthcare.com/healthcare/francis-collins-privacy-a-priority-for-precision-medicine-initiative. Accessed October 26, 2016.
12. MacDonald E. Cyber attacks on small businesses on the rise. April 27, 2016. Available at: http://www.foxbusiness.com/features/2016/04/27/cyber-attacks-on-small-businesses-on-rise.html Accessed October 26, 2016.
13. Allen A. Cyber ransom attacks panic hospitals, alarm Congress. July 18, 2016. Available at: http://www.politico.com/story/2016/07/cyber-ransom-attacks-panic-hospitals-congress-225791. Accessed October 26, 2016.
14. Nakashima E. Hacks of OPM databases compromised 22.1 million people, federal authorities say. July 9, 2015. Available at: https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/. Accessed October 26, 2016.
15. Klonoff DC, Kleidermacher DN. Now is the time for a cybersecurity standard for connected diabetes devices. *J Diabetes Sci Technol*. 2016;10(3):623-626.
16. Diabetes Technology Society. DTS cybersecurity standard for connected diabetes devices. Available at: https://www.diabetestechnology.org/dtsec.shtml. Accessed October 26, 2016.