Context Sensitive Health Informatics: Sustainability in Dynamic Ecosystems
R. Marcilly et al. (Eds.)

doi:10.3233/SHTI190156

Managing Privacy and Data Sharing Through the Use of Health Care Information Fiduciaries

Paul R. DEMURO [a, 1] and Carolyn PETERSEN [b]
[a] *Nelson Mullins Broad and Cassel, Ft. Lauderdale, FL, USA*
[b] *Mayo Clinic, Rochester, MN, USA*

Abstract. Policy and regulation seldom keep up with advances in technology. Although data de-identification is seen as a key to protecting one's data, re-identification is often possible. Whether one's data is to be used for care, research, or commercial purposes, individuals are concerned about the use of their information. The authors propose the concept of an information fiduciary for holders of data, describe how it might be applied in a health care context, and outline considerations to determine whether a holder of health care-related information should be regarded as an information fiduciary.

Keywords. Privacy, data sharing, health policy, de-identification, fiduciary

1. Introduction

An electronic health record (EHR) is the systemized collection of patient electronically-stored health information in digital format. Before EHRs came into wide use, when a patient visited a clinician, notes of that visit were generally kept in a paper record of some kind. The patient and the clinician were the key stakeholders in the encounter, the patient had an expectation of privacy and confidentiality in the relationship, and both patient and clinician expected the clinician to retain that privacy and confidentiality. De-identification of patient information was largely nonexistent because the information was not accessible without access to the paper record or the claim, and the form in which health information existed was not conducive to large-scale research. When a patient participated in a clinical trial, that person's data was used in the context of the trial, and recorded in some form, but generally the only information available was that which was accessed in the context of the clinical trial.

Today, protected health information (PHI) exists in multiple sources, including EHRs, and patient-generated health data (PGHD) that may be transmitted electronically to one's care team through fitness or other devices that can track additional information about an individual. Thus, the company hosting the EHR, the vendor of the data-creating devices, and third-party trackers are also stakeholders that have access to these data. In addition, individuals post information on social media, create health-related information (e.g., the number of steps taken per day, searching the Internet for flu remedies), and complete transactions that are not healthcare-related in nature (e.g., purchasing items at

[1] Corresponding Author: Paul R. DeMuro, Email: paul.demuro@nelsonmullins.com

a supermarket). Entities playing a role in these transactions are additional stakeholders that hold information about an individual that can be accessed in some form.

Policymakers and regulators seek to preserve the integrity of the patient-clinician relationship by enacting laws and regulations that protect the confidentiality associated with clinical encounters. However, such groups also desire to facilitate research that might benefit the common or public good and public health. Such researchers and research organizations and their funders, whether nonprofit or for-profit, are stakeholders, and policymakers and regulators may prioritize their interests in data to avoid stymieing or impeding technological developments, even if data commercialization could occur.

2. Protection of PGHD through De-Identification

De-identification of PGHD is one aspect of health policy in which regulators have attempted to direct commercial activity. The General Data Protection Regulation (GDPR) [1], which replaced the Data Protection Directive [2], applies to European Economic Area (EEA) member states and to companies that offer goods or services to European Union (EU) data subjects or monitor behavior of EU data subjects. The GDPR defines personal data broadly compared to the Health Information Portability and Accountability Act (HIPAA) [3] in that it includes identifying information of EEA health care providers, including institutional staff and individuals who are not study participants or patients. It also includes personal data of a data subject, noting what those identifiers might be, and special categories of personal data. The GDPR covers the processing and/or operations performed on personal data, and applies to controllers who are persons or entities that determine the purposes and means of processing personal data on behalf of the controllers. Even US entities can be subject to the GDPR when they interact with data that is subject to the GDPR [4].

Similarly, American policymakers enacted HIPAA and the Health Information Technology and Economic and Clinical Health Act (HITECH) [5] to manage use of health data. HIPAA contains privacy and security rules that provide protection for PHI that may be used or disclosed by providers, health plans, or data clearinghouses (also known as covered entities). These covered entities and their business associates are regulated, but not the data itself. Of particular importance is the fact that data which can be de-identified consistent with HIPAA's parameters are not protected by HIPAA; it is in this context that data can be used or sold for research and/or commercial purposes. HITECH was created to promote meaningful use of health IT and reinforce HIPAA privacy and security measures related to transmission of health information [6]. In addition, some US states also seek to regulate data use. In 2018 California passed its own form of GDPR-type legislation, the California Consumer Privacy Act, which includes portions of the GDPR and the ballot initiative from which it emanated [7].

However, policy and regulation seldom keep up with the advances in technology, among them data de-identification [8]. In addition, different jurisdictions have different laws and regulations, which often overlap or are inconsistent. In the global economy, innovations rarely are put into use in just one jurisdiction. Thus, when policymakers and regulators promulgate law and regulations on how to de-identify data, as with HIPAA, such laws and regulations can become outdated. Though some stakeholders seek to de-identify data in accordance with applicable law and regulations or validate that they have done so correctly, others actively attempt to re-identify what was thought to be de-

identified data, and review of re-identification attacks indicates that approximately 25% were successful as of 2015 [9].

Clearly, a balance of the interests of patients, clinicians, hospitals, and payers with those of researchers and commercial entities must be achieved. It may be argued that if the de-identification of data might lead to advances for the public good, for example through improved public health measures that benefit society as a whole, there should be greater tolerance for data re-identification than if it would lead to the development of a commercial product. However, that commercial product might result in something that is more readily available to all (e.g., through investment in the company). In this regard, at the risk of adding another layer of regulation on the already numerous layers of regulations, one can expand the notion of "information fiduciary" from the setting of search engines and social media platforms to the above stakeholders, thereby holding them to a higher standard that currently exists.

3. Data Holder as Fiduciary

A fiduciary is an individual or an entity that holds another's information in trust. For example, financial advisors are fiduciaries. An information fiduciary, thus, is an entity that holds personal information in some protected way [10]. Given that the law does not seem to keep up with technological advances and following existing law (including de-identification requirements) and company privacy policies may be insufficient to protect personal data, the concept of "information fiduciaries" may offer a useful framework for analysis. Even if there is an opportunity to "consent" to what a company might do with one's data, one must consider whether the consent was truly volitional and whether the person really knew what he or she might be consenting to. One could argue that in the context of health care, one's consent to use one's data is even less volitional than with social media or search engines because one may be unable to live without medical care.

In determining whether one or an entity might be considered an information fiduciary, a number of questions should be considered. Initially, the kind of information should be identified (e.g., from an EHR, personal device that creates PGHD). It may be important to ascertain how the information was generated. Other considerations include who is/are the intended recipient(s) of such information, to whom the information was actually transmitted, and the purpose of the data transmittal. A more thorny issue might be who owns the data, given that there might be more than one owner, and one might own it as the initial data (e.g., a patient), but another in a different form (e.g., a patient record). The nature and extent of any consent processes and disclosure agreements completed for the use of the data also should be taken into account.

Whether one should be treated as an information fiduciary depends upon what benefits might be derived from the use of the data, and whether those benefits inure to the public good or if they are commercial in nature, where only the holder of the data benefits financially and otherwise. That could include a company developing an algorithm which uses artificial intelligence and machine learning for which the company obtains intellectual property protection, and makes millions of dollars. If a financial advisor makes more money by selling a client financial products rather than by managing the individual's overall financial situation, questions would be raised about whether the financial advisor is really a fiduciary. Similarly, if an individual or entity is to be considered as a potential information fiduciary, consideration must be given to whether they would benefit financially from an individual's information without the individual's

full knowledge and consent and without some benefit inuring to the individual, whether directly or indirectly.

Another important consideration should be to whom is the data transmitted. Individuals may have less of an expectation of privacy and confidentiality when information is placed on social media for others to see than when one conducts a search on Google. An individual would have even a greater expectation of privacy and confidentiality when their data are communicated to their medical care team.

At a broader level, also meriting consideration is the value of the data and whether the original patients whose data is used will receive some benefit. In this context, it will be important to analyze any legal considerations and whether the data is truly de-identified or has been subject to pseudomynization. Who made these determinations and the potential means of re-identifying the data and the possibility of doing so are other relevant concerns.

4. Ethical Considerations

It is important that those individuals and entities who would be within the ambit of an information fiduciary comply not only with all applicable laws and regulation, but also ethical considerations. In fact, given the special relationship that they are in, they should go beyond legal and ethical considerations. Given the special nature of an information fiduciary, this individual or organization should not merely determine whether data has been de-identified or subject to pseudomynization in accordance with applicable law and regulation, but should also try to anticipate whether the data might later be re-identified. Data sets are dynamic in nature and additional information might be added later that would increase the likelihood of re-identification. Advances in technology too might make reverse engineering the data de-identification process possible later.

Some guidelines to consider in determining whether a holder of health care-related data, including PGHD, should be regarded as a health care information fiduciary include the following:

- Does the individual whose data is generated have an expectation of privacy and confidentiality with respect to that data?
- How sensitive might the individual believe his or her data is?
- Was the form in which the data was transmitted such that an individual would reasonably expect that it would only be received and used by the party intended?
- Will the data be used to provide better care for the individual whose data it is, or be for the common or public good, or will it be commercialized for the good of the holder of the data?
- Would the individual whose data it is have consented to the eventual use, if it knew what that use was?
- What is the value of the data?
- Can the data truly be de-identified and not re-identified?

The answer to most of these questions typically will indicate whether an individual or entity holding health care-related data should be treated as a health care information fiduciary. As such, additional research is necessary to try to better define the parameters of healthcare information fiduciaries and provide guidance in this evolving area.

Having the holder of one's personal data be a fiduciary or at least have the relationship governed by some sense of responsibility and protection for the individual's data offers obvious advantages. Of course, defining what that sense of responsibility and protection might be can be quite difficult and depend upon the answers to the questions posed previously. One might look to traditional notions of privacy and confidentiality to explore what an individual's expectation might be for his or her data. Most likely, some data (e.g., whether a person has a communicable disease) will be much more sensitive than other data (e.g., one's height). An individual's expectations about privacy and confidentiality might also depend upon how the information is generated and transmitted. For example, one might have less of an expectation of privacy and confidentiality about the number of steps on one's fitness tracker than their genetic information.

5. Conclusion

Protected health information exists in multiple sources, including as data generated by patients for their own health-related uses, and it can be transmitted and shared in numerous ways. Patients, citizens, clinicians, researchers, payers, health care administrators, policymakers, and others have variable expectations of privacy with respect to such data, though most can agree on the importance of protecting patients' privacy and managing access to PHI appropriately. Although de-identification of data prior to non-care-related uses is seen as important, the limitations of data de-identification have become apparent and other approaches to the maintenance of privacy are needed. The health care information fiduciary offers one such option.

Given the possibilities for data re-identification, for uses of it for purposes not intended by the original holder of the data, and for its commercialization without benefit to such individuals, there is potential for ultimate holders of protected health information to be considered as health care information fiduciaries with the responsibility of holding such information in trust. This article provides guidelines for determining whether a holder of health-related data should be regarded as a health care information fiduciary.

Initial steps to explore the potential use(s) of health care information fiduciaries should focus on what might be done to minimize health care information fiduciaries from using personal data in ways not intended by the individuals to whom data pertain. Structures that prevent health care information fiduciaries from benefiting from such data use unless it is for the common good or the public or unless there are other extenuating circumstances are needed. In addition, standards should be developed for information fiduciaries, including a code of conduct that would be dynamic in nature.

Beyond these efforts, further work should emphasize determination of practice standards and policy changes needed to establish and regulate fiduciaries, and to create mechanisms for enforcement, recognizing that standards and policies may need to change from time to time. Perhaps policymakers and legislatures should focus on what might happen to such individual data in the future, rather than considering only what has happened in the past as they create a regulatory infrastructure.

References

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of

such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504 (accessed Feb 8, 2019).
[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (1995). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 (accessed Feb 8, 2019).
[3] Summary of the HIPAA privacy rule, U.S. Department of Health and Human Services, (2013). https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (accessed Feb 8, 2019).
[4] J. Raines, A. Laughton, S. Shaw, and A. Thomas, The broad reach of the GDPR: Europe's new data protections and their impact on U.S. health care entities, *AHLA Connections* **23** (2019), 10-14.
[5] 45 CFR Part 160: HIPAA Administrative Simplification: Enforcement, U.S. Department of Health and Human Services, (2009). https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf (accessed Feb 8, 2019).
[6] HITECH Act Enforcement Interim Final Rule, U.S. Department of Health and Human Services, (2017). https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html (accessed Feb 8, 2019).
[7] Assembly Bill No. 375: California Consumer Privacy Act, State of California, (2018). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (accessed Feb 8, 2019).
[8] W.N. Price II, M.E. Kaminski, T. Minssen, K. Spector-Bagdady, Shadow health records meet new data privacy laws, *Science* **363** (2019), 448-450.
[9] K. El Emam, E. Jonker, L. Arbuckle, B. Malin, A systematic review of re-identification attacks on health data, *PLoS One* **6** (2011), e28071.
[10] J. Zittrain, Facebook could decide an election without anyone ever finding out, *The New Republic* (2014).