Privacy and Security Issues with Mobile Health Research Applications

Stacey A. Tovino

Introduction

This article examines the privacy and security issues associated with mobile application-mediated health research, concentrating in particular on research conducted or participated in by independent scientists, citizen scientists, and patient researchers. Building on other articles in this issue that examine state research laws and state data protection laws as possible sources of privacy and security protections for mobile research participants,[1] this article focuses on the lack of application of federal standards to mobile application-mediated health research. As discussed in more detail below, the voluminous and diverse data collected by some independent scientists who use mobile applications to conduct health research may be at risk for unregulated privacy and security breaches,[2] leading to dignitary, psychological, and economic harms for which participants have few legally enforceable rights or remedies under current federal law.[3] Federal lawmakers may wish to consider enacting new legislation that would require otherwise unregulated health data holders to implement reasonable data privacy, security, and breach notification measures.

Background

Privacy and security are fundamental aspects of the ethical conduct of research involving human participants. Adopted by the World Medical Association (WMA) in 1964, the Declaration of Helsinki established a duty of physicians who are involved in medical research to protect "privacy … and confidentiality of personal information of research subjects."[4] Consistent with the mandate of the WMA, the Declaration of Helsinki is addressed primarily to physician-researchers,[5] but it also "encourages others who are involved in medical research involving human subjects to adopt these principles."[6]

First prepared by the Council for International Organizations of Medical Sciences (CIOMS) in collaboration with the World Health Organization in 1982, the International Ethical Guidelines for Health-Related Research Involving Humans (Guidelines) address the use of "data obtained from the online environment and digital tools."[7] In particular, the current (2016) Guidelines provide:

> When researchers use the online environment and digital tools to obtain data for health-related research they should use privacy-protective measures to protect individuals from the possibility that their personal information is directly revealed or otherwise inferred when datasets are published, shared, combined or linked. Researchers should assess the privacy risks of their research, mitigate these risks as much as possible and describe the remaining risks in the research protocol. They should anticipate, control, monitor and review interactions with their data across all stages of the research.[8]

The Guidelines also state that researchers should, through an "opt-out procedure," inform persons whose data may be used in the context of research in the online environment of the purpose and context of the intended data uses, the privacy and security measures used to protect such data, and the limitations of the measures used and the privacy risks that may

Stacey A. Tovino, J.D., Ph.D., *is the Judge Jack and Lulu Lehman Professor of Law at the William S. Boyd School of Law, University of Nevada-Las Vegas.*

The Journal of Law, Medicine & Ethics, 47 S2 (2019): 154-158. © 2019 The Author(s)
DOI: 10.1177/1073110520917041

https://doi.org/10.1177/1073110520917041 Published online by Cambridge University Press

remain despite the implementation of safeguards.[9] If a person objects to the use of his or her data for research purposes, the Guidelines would forbid the researcher from using that data.[10]

The Common Rule

In addition to the ethical principles set forth in the Declaration of Helsinki and the Guidelines, the Federal Policy for the Protection of Human Subjects (the Common Rule) requires institutional review boards that review and approve research funded by a signatory agency to determine, when appropriate, that "adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data" exist.[11] Because many independent scientists, citizen scientists, and patient researchers do not receive federal funding and do not work for an institution that receives federal funding, the Common Rule's confidentiality and privacy provisions are inapplicable to their research.[12]

The voluminous and diverse data collected by some independent scientists who use mobile applications to conduct health research may be at risk for unregulated privacy and security breaches, leading to dignitary, psychological, and economic harms for which participants have few legally enforceable rights or remedies under current federal law. Federal lawmakers may wish to consider enacting new legislation that would require otherwise unregulated health data holders to implement reasonable data privacy, security, and breach notification measures.

The HIPAA Rules

The HIPAA Privacy, Security, and Breach Notification Rules, promulgated by HHS pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH),[13] provide standards that may be used as a reference point for considering the future regulation of mobile application-mediated health research. As background, the HIPAA Rules were designed to protect the privacy and security of individually identifiable health information created, obtained, or maintained in certain health care and health insurance contexts and to assist patients and insureds in protecting themselves in the event of a privacy or security breach.[14] Although HIPAA authorizes the federal government to impose civil and criminal penalties for violations of the HIPAA Rules,[15] the HIPAA Rules are limited in application to: (1) health plans, health care clearinghouses, and those health care providers that transmit health information in electronic form in connection with standard transactions, including health insurance claims (covered entities);[16] and (2) persons or entities that access or use protected health information (PHI) to provide certain services to, or to perform certain functions on behalf of, covered entities (business associates).[17]

As currently written, the HIPAA Rules do not regulate a number of individuals and institutions that collect, use, or disclose PHI, including many independent scientists, citizen scientists, and patient researchers as well as some mobile app developers and data storage companies that support them.[18] The HIPAA Rules may, however, be used as a reference point for considering the future regulation of non-HIPAA covered entities that conduct research. For example, the HIPAA Privacy Rule requires covered entities to adhere to certain use and disclosure requirements,[19] individual rights requirements,[20] and administrative requirements[21] during the conduct of research. In particular, covered researchers must obtain prior written authorization from each research participant before using or disclosing the participant's PHI unless the use or disclosure falls into one of four research-related exceptions to the authorization requirement.[22]

Although much has been made of the concern that some individuals do not read or understand authorizations and other types of mandated forms and disclosures,[23] this concern does not obviate the ethical obligation of a researcher, regardless of whether the researcher is affiliated or independent, to request permission to use an individual's data for research and to respect the individual's decision.[24] For these reasons, future regulations governing independent, mobile application-based research should be guided by a principle that is analogous to the HIPAA Privacy Rule's authorization requirement. That is, independent scientists should obtain some form of prior writ-

The Journal of Law, Medicine & Ethics, 47 S2 (2019): 154-158. © 2019 The Author(s)

https://doi.org/10.1177/1073110520917041 Published online by Cambridge University Press

ten permission from prospective research participants to use and disclose their data for current and future research purposes.[25]

The HIPAA Privacy Rule requires research authorizations to contain a number of core elements and required statements.[26] Most of these elements and statements are relevant to the context of independent, mobile app-based research and could be included in electronic authorization forms signed by prospective research participants. These elements and statements would include, but not be limited to: (1) the name or other specific identification of each mobile application-mediated researcher who will be collecting, using, or disclosing the research participant's data; (2) the name or specific identification of each person who will be receiving the participant's data from the researcher, including any backend data collectors, data processors, and other researchers; (3) a specific and meaningful description of data relating to the participant that will be collected by the mobile application; (4) a specific description of the current research project for which the participant's data will be collected, used, or disclosed; (5) if the researcher expects to use or disclose the individual's data for future research projects, information sufficient to put the individual on notice of that expectation;[27] (6) a specific expiration date or a relevant expiration event after which the individual's data will no longer be collected, used, or disclosed; (7) a description of the right of the individual to revoke the authorization together with the exceptions to the right to revoke, including situations in which the individual's data has already been collected, used, or disclosed for research; and (8) the electronic signature of the individual.[28] Conventional researchers who use mobile applications to conduct federally-regulated health research have already considered how best to deliver HIPAA-mandated disclosures to remote research participants.[29] These online processes could be adapted by independent researchers as well.

The HIPAA Security Rule also may be used as a reference point for considering options for the future regulation of independent, mobile application-based research. The HIPAA Security Rule requires covered researchers to adhere to certain administrative,[30] physical,[31] and technical[32] safeguards designed to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI) and to protect against reasonably anticipated threats or hazards to the security and integrity of ePHI.[33] Administrative requirements include designating a security official who is responsible for the development and implementation of the covered entity's security policies and procedures[34] and implementing policies and procedures that prevent, detect, contain, and correct security violations; ensuring that workforce members have appropriate access to ePHI; preventing workforce members who should not have access to ePHI from obtaining such access; creating a security awareness and training program for all workforce members; and addressing and responding to security incidents, emergencies, environmental problems, and other occurrences such as fire, vandalism, system failure, and natural disaster that affect systems containing ePHI and the security of ePHI, among other requirements.[35]

The HIPAA Security Rule's physical safeguard provisions require covered entities to implement policies and procedures that limit physical access to electronic information systems and the facilities in which they are located; address the safeguarding, functioning, and physical attributes of workstations through which ePHI is accessed; and govern the receipt and removal of hardware and electronic media that contain ePHI.[36] Finally, the HIPAA Security Rule's technical safeguards require covered entities to implement policies and procedures that allow access to ePHI only to those persons or software programs that have been granted access rights; hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI; policies and procedures to protect ePHI from improper alteration or destruction; procedures to verify that a person or entity seeking access to ePHI is the one claimed; and technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.[37] In addition to its Privacy and Security Rules, HHS also has promulgated a Breach Notification Rule.[38] Following the discovery of a breach[39] of unsecured protected health information (uPHI),[40] covered entities are required to notify each individual whose uPHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.[41] The purpose of this notification is to give individuals the opportunity to protect themselves from economic, dignitary, and psychological harms that may follow from the data breach.

In light of the ethical and legal principles discussed above, Congress and appropriate federal agencies should consider requiring reasonable privacy, security, and breach notification measures during the conduct of mobile application-mediated health research. Reasonable privacy measures might include, for example: (1) requiring unregulated researchers to anonymously report their study results; (2) providing that if research data includes participant names or other individual identifiers, these should not be reported or otherwise disclosed; (3) prohibiting marketing and

The Journal of Law, Medicine & Ethics, 47 S2 (2019): 154-158. © 2019 The Author(s)
https://doi.org/10.1177/1073110520917041 Published online by Cambridge University Press

other commercial secondary uses of mobile application-mediated research data without the prior, explicit consent of each research participant; (4) prohibiting "click-through" or other non-explicit, non-meaningful forms of consent; (5) requiring that unregulated researchers implement reasonable administrative, physical, and technical safeguards designed to protect the security of participant data, such as requiring unregulated researchers to safeguard their physical equipment from unauthorized access, tampering, or theft, and encrypting their research data or otherwise make such data unintelligible to unauthorized users; and (6) requiring unregulated researchers to promptly notify their research participants in the event of a discovery of a data breach.

Conclusion

Current federal laws that contain data privacy and security standards do not apply to many independent scientists, citizen scientists, and patient researchers who conduct mobile application-mediated research. As a result, the voluminous and diverse data collected in this context may be at risk for privacy and security breaches, leading to dignitary, psychological, and economic harms for which research participants have few legally enforceable rights or remedies under current federal law. Congress and appropriate federal agencies should consider requiring reasonable privacy, security, and breach notification measures during the conduct of otherwise unregulated research. The HIPAA Rules, although outdated in terms of their limited application, offer an illustrative reference point for considering new privacy and security legislation or regulation. Newly introduced federal bills including the Smartwatch Data Act, the Mind Your Own Business Act, and the Protecting Personal Health Data Act offer illustrative options for implementing privacy and security measures applicable to otherwise unregulated health researchers and other data holders.

Acknowledgment

Research on this article was funded by the following grant: Addressing ELSI Issues in Unregulated Health Research Using Mobile Devices, No. 1R01CA20738-01A1, National Cancer Institute, National Human Genome Research Institute, and Office of Science Policy and Office of Behavioral and Social Sciences Research in the Office of the Director, National Institutes of Health, Mark A. Rothstein and John T. Wilbanks, Principal Investigators.

Note

The author has no conflicts of interst to disclose.

References

1. *See* S.A. Tovino, "Mobile Research Apps and State Research Laws," *Journal of Law, Medicine & Ethics* 48, Supp. 1 (Supp.) (2020): 82-86; S.A. Tovino, "Mobile Research Apps and State Data Protection Statutes," *Journal of Law, Medicine & Ethics* 48, Supp. 1 (2020): 87-93.
2. *See, e.g.*, Z. Tufekci, "The Latest Data Privacy Debacle," *New York Times*, January 30, 2018 (discussing Strava, the mobile exercise application that inadvertently revealed the secret locations of American military bases and service members); *Opperman v. Path, Inc.*, 205 F.Supp.3d 1064, 1073 (N.D. Cal. 2016) (explaining that the Yelp mobile application exceeded the scope of its users' consent when it uploaded its users' contacts data without explicit permission).
3. *See, e.g.*, M.A. Rothstein, "Ethical Issues in Big Data Health Research," *Journal of Law, Medicine & Ethics* 43, no. 2 (2015): 425-428. (discussing the psychological and dignitary harms that are associated with the loss of privacy in the context of big data health research).
4. World Medical Association, *Declaration of Helsinki*, General Principles, ¶ 9 (1964).
5. *Id.*, Preamble, ¶ 2.
6. *Id.*
7. Council for International Organizations of Medical Sciences, *International Ethical Guidelines for Health-Related Research Involving Humans*, Guideline 22 (4th ed. 2016) ("Use of Data Obtained from the Online Environment and Digital Tools in Health-Related Research").
8. *Id.*
9. *Id.*
10. *Id.*
11. 45 C.F.R. § 46.111(a)(7).
12. *See* M.A. Rothstein, J.T. Wilbanks, and K.B. Brothers, "Citizen Science on Your Smartphone: An ELSI Research Agenda," *Journal of Law, Medicine & Ethics* 43, no. 2 (2015): 897-902. (explaining that virtually all American academic and health care institutions that conduct human subjects research are regulated by the Common Rule but that "research undertaken by independent entities or individuals, including citizen scientists, is not subject to the Common Rule.").
13. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 42 U.S.C.) [hereinafter HIPAA], amended in part by Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 115, 226 (codified as amended in scattered sections of 42 U.S.C.) [hereinafter HITECH]. HHS's privacy regulations, which implement section 264(c) of HIPAA, are codified at 45 C.F.R. Part 164, Subpart E (45 C.F.R. §§ 164.500-.534). HHS's security regulations, which implement section 262(a) of HIPAA [42 U.S.C. § 1320d–2(d)(1)], are codified at 45 C.F.R. Part 164, Subpart C (45 C.F.R. §§ 164.302-.318). HHS's breach notification regulations, which implement section 13402 of HITECH [42 U.S.C. § 17932], are codified at 45 C.F.R. Part 164, Subpart D (45 C.F.R. §§ 164.400-.414).
14. *See* 45 C.F.R. §§ 164.500-.534, §§ 164.302-.318, and §§ 164.400-.414 (setting forth the privacy, security, and breach notification obligations of covered entities and business associates under the HIPAA Rules).
15. *See* HIPAA, *supra* note 13, § 242 (adding 42 U.S.C. § 1320d-5 (establishing civil penalties for violations of the HIPAA Rules); 42 U.S.C. § 1320d-6 (establishing criminal penalties for violations of the HIPAA Rules); HITECH, *supra* note 13, § 13410(d) (revising the amount of the civil penalties authorized by HIPAA).
16. *See* 45 C.F.R. § 160.103 (defining covered entity); *id.* § 160.102(a) (applying the HIPAA Rules to covered entities).
17. *See id.* § 160.103 (defining business associate); *id.* § 160.102(b) (applying the HIPAA Rules to business associates).
18. *See*, e.g., N.P. Terry and T.D. Gunter, "Regulating Mobile Mental Health Apps," *Behavioral Sciences and the Law* 36, no. 1 (2018): 136-144. ("[Mobile medical applications] tend to be developed outside of traditional health care spaces with the result that they exist in a lightly regulated, 'HIPAA-free zone.'"); Rothstein, Wilbanks and Brothers, *supra* note 12 ("[R]esearch undertaken by an individual or entity that is

The Journal of Law, Medicine & Ethics, 47 S2 (2019): 154-158. © 2019 The Author(s)

https://doi.org/10.1177/1073110520917041 Published online by Cambridge University Press

not a HIPAA-covered entity, such as a citizen scientist, is not required to follow federal privacy rules); M.A. Rothstein, "The End of the HIPAA Privacy Rule?" *Journal of Law, Medicine & Ethics* 44, no. 2 (2016): 352-358 ("Among the reasons for the Privacy Rule's disrepute, especially among privacy advocates, is its limited coverage; it applies only to 'covered entities'…"); I.G. Cohen and M.M. Mello, "HIPAA and Protecting Health Information in the 21st Century," *JAMA Online First*, May 24, 2018 ("HIPAA attaches (and limits) data protection to traditional health care relationships and environments. The reality …is that HIPAA-covered data form a small and diminishing share of the health information stored and traded in cyberspace."); I.G. Cohen and M.M. Mello, "Big Data, Big Tech, and Protecting Patient Privacy," *JAMA Online First*, August 9, 2019 ("HIPAA is a 20th-century statute ill equipped to address 21st-century data practices.").

19. 45 C.F.R. §§ 164.502-.514.
20. *Id.* §§ 164.520-.528.
21. *Id.* § 164.530.
22. *Id.* § 164.508(a)(1) (establishing the prior written authorization requirement); *id.* § 164.512(i)(1)(i)-(iii) (establishing three research-related exceptions to the authorization requirement); *id.* § 164.514(e) (establishing a fourth research-related exception to the authorization requirement involving research uses and disclosures of limited data sets).
23. *See, e.g.*, O. Ben-Shahar and C.E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (2014) (arguing that mandated disclosures routinely fail to achieve their desired goals).
24. *See, e.g.*, M.A. Rothstein, "Improve Privacy in Research by Eliminating Informed Consent? IOM Report Misses the Mark," *Journal of Law, Medicine & Ethics* 37, no. 3 (2009): 507-512 (arguing that a recommendation of the Institute of Medicine that would automatically convert all patients into research subjects without their knowledge or consent denigrates respect for autonomy).
25. *But see* Cohen and Mello, "Big Data, Big Tech, and Protecting Patient Privacy," *supra* note 18 ("Patients could be presented with a blanket 'front door' authorization form and choose to sign or withhold permission. However, this approach may prove to be mere ethical window dressing. HIPAA appropriately calls such a process authorization, not consent, because patients are rarely given the information and opportunity to ask questions needed to give meaningful informed consent to future uses of their data. Even if those problems could be overcome, it is asking a great deal of patients to imagine and assess how their information may be used and what the risk of re-identification may be.") (internal references and citations omitted).
26. 45 C.F.R. § 164.508(c)(1)-(2) (listing the core elements and required statements of a HIPAA-compliant authorization form).
27. *See* U.S. Dep't Health & Human Servs., *Guidance on HIPAA and Individual Authorization of Uses and Disclosures of Protected Health Information for Research 21st Century Cures Act of 2016 Mandate* (June 2018) (responding to the 21st Century Cures Act's mandate that the Secretary of HHS publish guidance regarding future research authorizations).
28. 45 C.F.R. § 164.508(c)(1)-(2).
29 *See* S. Moore et al., "Consent Processes in Mobile App Mediated Research: Systematic Review," *Journal of Medical Internet Research mHealth and uHealth* 5, no. 8 (2017): E126 (showing how Duke University uses a mobile research application to deliver mandated disclosures to remotely located research participants and to obtain their electronic signatures).
30. 45 C.F.R. § 164.308.
31. *Id.* § 164.310.
32. *Id.* § 164.312.
33. *Id.* § 164.306(a)(1)-(2).
34. *Id.* § 164.308.
35. *Id.*
36. *Id.* § 164.310.
37. *Id.* § 164.312.
38. *Id.* §§ 164.400-.414.
39. *Id.* § 164.402 (defining breach).
40. *Id.* (defining uPHI).
41. *Id.* § 164.404(a)(1).

The Journal of Law, Medicine & Ethics, 47 S2 (2019): 154-158. © 2019 The Author(s)

https://doi.org/10.1177/1073110520917041 Published online by Cambridge University Press