HHS Public Access

Author manuscript

Circulation. Author manuscript; available in PMC 2021 February 25.

Published in final edited form as:

Circulation. 2020 February 25; 141(8): 613–615. doi:10.1161/CIRCULATIONAHA.119.044966.

Privacy Gaps for Digital Cardiology Data: Big Problems with Big Data

Jessica R. Golbus, MD, MS[1], **W. Nicholson Price II, JD, PhD**[2,3,4], **Brahmajee K. Nallamothu, MD, MPH**[1,5,6]

[1]Division of Cardiovascular Diseases, Department of Internal Medicine, University of Michigan, MI.

[2]University of Michigan Law School, Ann Arbor, MI, USA.

[3]Project on Personalized Medicine, Artificial Intelligence, & Law, Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics, Cambridge, MA, USA.

[4]Center for Advanced Studies in Biomedical Innovation Law, University of Copenhagen, Copenhagen, Denmark.

[5]Michigan Integrated Center for Health Analytics and Medical Prediction (MiCHAMP) and Division of Cardiovascular Diseases, Department of Internal Medicine, University of Michigan, MI.

[6]The Center for Clinical Management and Research, Ann Arbor VA Medical Center, MI.

Abstract

Mr. M is a 55 year-old man who suffers an acute myocardial infarction (MI) and undergoes coronary stenting. Following hospitalization, he completes cardiac rehabilitation. Thereafter, he is approached about joining a digital smartwatch study to help monitor his health behaviors. He enrolls with enthusiasm, and, feeling empowered, creates a profile on PatientsLikeMe to share lessons from his medical journey. There he reads about an over-the-counter vitamin and downloads a coupon for his local supermarket. Determined to remain accountable for his health, he starts exercising with a fitness trainer and provides her with heart rate data from his smartwatch. He also downloads a mobile nutrition application she recommends.

Rapid growth in our information economy – spurred by advancements in digital technology and artificial intelligence – is expanding the amount and type of data collected in healthcare. [1] While the Health Information and Privacy Protection Act (HIPAA) Privacy Rule regulates inappropriate sharing of protected health information (PHI), a substantial amount of health-related data are outside its purview and unregulated in the US. HIPAA's narrow scope is

Corresponding Author: Jessica R. Golbus MD, MS, University of Michigan Health System, 2381 CVC SPC 5853, 1500 E. Medical Center Drive, Ann Arbor, MI 48109-5853, Phone: 734-936-8214, Fax: 734-615-3326, jgolbus@med.umich.edu.

Conflict of Interest Disclosures: Dr. Nallamothu is a principal investigator or co-investigator on research grants from the NIH, VA HSR&D, the American Heart Association, Apple, Inc, and Toyota. He also receives compensation as Editor-in-Chief of Circulation: Cardiovascular Quality & Outcomes, a journal of the American Heart Association. Finally, he is a co-inventor on U.S. Utility Patent Number US15/356,012 (US20170148158A1) entitled "Automated Analysis of Vasculature in Coronary Angiograms" that uses software technology with signal processing and machine learning to automate the reading of coronary angiograms, held by the University of Michigan. The patent is licensed to AngioInsight, Inc., in which Dr. Nallamothu holds ownership shares (although it has yet to be funded).

especially apparent in the marketplace, where users and uses of health-related data have expanded far beyond what HIPAA's drafters initially anticipated. We believe investigators and clinicians need to be aware of these privacy challenges when recommending digital technology for their patients. Although the growing availability of "Big Data" may empower patients, it can also lead to commercial exploitation and privacy harms.

HIPAA and the Privacy Rule.

HIPAA, introduced in 1996, and its associated Privacy Rule, finalized in 2000, establish rights of individuals with respect to use and disclosure of their health information.[1] HIPAA focuses on regulating custodians of data, so called "covered entities," that include providers, healthcare systems, health insurers, and their business associates.[2] HIPAA regulates covered entities' use of PHI for both clinical care and research.[1] Information that is de-identified is not protected under HIPAA, nor is the behavior of non-covered entities who might produce or process health-related information. Thus, while HIPAA protects certain data and individuals, a large fraction of health-related data and entities remains unregulated.

Contemporary Challenges for Health-Related Data.

It has become increasingly evident that health-related data outside of HIPAA's jurisdiction can be highly personal and, at times, re-identifiable. This results not only from the generation and dissemination of data by non-covered entities but also from the triangulation of health-related data with other sources of information and their application to predictive analytics, which can identify novel correlations within data.[3] These issues now arise during many scenarios encountered in routine care. For example, Mr. M's participation in a digital smartwatch study clearly falls under the umbrella of HIPAA. But below are three common ways his interactions with websites, businesses, and non-medical health providers may impact his health-related data outside of HIPAA's jurisdiction.

Mobile Device Data.

Patients frequently share data from mobile devices (e.g., phones, smartwatches) with non-covered entities, often unaware of downstream uses of that data. One recent study of 24 prominent, medically-related mobile applications found that 19 shared user data with 55 unique entities.[4] In the case of Mr. M, smartwatch data he shared with his trainer or nutrition application are not protected by HIPAA. In one scenario, his smartphone-based location tracking could be used to estimate the frequency of visits to fast food restaurants, a technique called geofencing. That information could then be combined with smartwatch data to make predictions. Not surprisingly, the boundary between simple digital data and highly sensitive health information can be crossed quite quickly.

Online Data.

Large amounts of data also enter the health ecosystem from patients' online activity. A rich picture of health could be painted through triangulation of information from internet search terms, medical blogs, online symptom checkers, and even donations to medical advocacy groups.[5] An intensely personal story of battling post-MI depression, shared online through

health websites like PatientsLikeMe, could be leveraged by third parties.[3] For others, third parties could glean insight into diagnoses like depression by recording online searches for "light therapy lamps" or "liked" posts from other patients with depression on social media websites such as Facebook. All of these interactions create an effluent of unregulated data that could lead to privacy harms.

Role of Commercial Entities.

This situation is further amplified by the intersection of mobile device and online data with commercial entities. The expanding number of unregulated stakeholders includes data brokers, advertising agencies, internet search engines, prescription drug monitoring companies, supermarkets, home testing laboratories, and credit card companies.[3] Mr. M's purchases of over-the-counter vitamins, recorded by the supermarket and his credit card company, could be sold to many of these entities including data aggregators under companies like Google, Facebook, and Amazon. Although patients may opt out, privacy policies may be unintelligible, as many are written at a college level.[5] Furthermore, when data are combined with advanced predictive analytics that information could be used to generate health scores that inform loan eligibility, life or disability insurance coverage, and even employment.[3] While regulations outside of HIPAA govern against discrimination using health diagnoses in some circumstances, exploiting non-health correlates may not violate US law.

Charting a Path Forward.

The confluence of growing health-related data, increased computing power, new technology, and new stakeholders creates both opportunities and challenges for providers and researchers interested in leveraging digital tools for clinical care. This can be particularly difficult to navigate, however, given a relative paucity of legislative or normative controls over the data. As healthcare providers, we believe two important areas need to be addressed to protect our patients' data.

First, we have an obligation to educate ourselves on safe and effective use of digital technology. This is especially important to allow for honest conversations with our patients around privacy issues, especially as we enroll them in clinical studies. Patients may mistakenly assume, for example, that physiologic data collected by mobile applications fall within the jurisdiction of HIPAA since that same information, when used for clinical care, is protected.[5] Second, we believe that greater legislation surrounding the use of health information is necessary. In 2018, the European Union (EU) began to enforce the General Data Protection Regulation (GDPR) which applies to all potentially identifiable personal data and mandates strengthened consent, with easily accessible and understandable forms; pre-specified use of data; some protection outside the EU; and individuals' rights to obtain their data or have their data erased. While we do not regard the GDPR as a panacea, the US does need law which (1) governs data, not just a limited number of covered entities that hold it; and (2) embraces a broad and inclusive definition of health-related data, without the artificial distinctions inherent in HIPAA. Legislation should not simply fixate on issues of consent, which places an unreasonable responsibility on consumers.

Despite the challenges that lie ahead for digital data, we believe the benefits these tools afford outweigh their risks and help us empower our patients. This balance, however, will shift if we do not practice "preventive medicine" and ensure that data are used responsibly and in the best interests of our patients.

Acknowledgements:

Dr. Golbus is supported by grant number T32-HL007853 from the NIH. Dr. Price is supported by Novo Nordisk Foundation NNF17SA0027784 and NCI grant 1 R01 CA214829-01A1.

References.

1. US Department of Health & Human Services. "Research." 4 3, 2003 https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html. Accessed September 28, 2019.
2. Price WN, 2nd and Cohen IG. Privacy in the age of medical big data. Nat Med. 2019;25:37–43. [PubMed: 30617331]
3. US Department of Health & Human Services. "Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges." A Report for the National Committee on Vital and Health Statistics (NCVHS) and its privacy, Security, and Confidentiality Subcommittee. 12 13, 2017 https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf. Accessed September 19, 2019.
4. Grundy Q, Chiu K, Held F, Continella A, Bero L and Holz R. Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. BMJ. 2019;364:l920. [PubMed: 30894349]
5. Glenn T and Monteith S. Privacy in the digital world: medical and health data outside of HIPAA protections. Curr Psychiatry Rep. 2014;16:494. [PubMed: 25218603]