HEALTH INFORMATION PRIVACY LAWS IN THE DIGITAL AGE: HIPAA DOESN'T APPLY

Posted on December 7, 2020 by Matthew

Category: Winter 2021

Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply

By Kim Theodos, JD, MS, RHIA, and Scott Sittig, PhD, MHI, RHIA

Abstract

The notion of health information privacy has evolved over time as the healthcare industry has embraced technology. Where once individuals were concerned about the privacy of their conversations and financial information, the digitization of health data has created new challenges for those responsible for ensuring that patient information remains secure and private. Coupled with the lack of updated, overarching legislation, a critical gap exists between advancements in technology, consumer informatics tools and privacy regulations.

Almost twenty years after the HIPAA (Health Insurance Portability and Accountability Act) compliance date, the healthcare industry continues to seek solutions to privacy challenges absent formal contemporary law. Since HIPAA, a few attempts have been made to control specific aspects of health information including genetic information and use of technology however none were visionary enough to address issues seen in today's digital data focused healthcare environment. The proliferation of digital health data, trends in data use, increased use of telehealth applications due to COVID-19 pandemic and the consumer's participatory role in healthcare all create new challenges not covered by the existing legal framework. Modern efforts to address this dilemma have emerged in state and international law though the United States healthcare industry continues to operate under a law written two decades ago. As technology continues to advance at a rapid pace along with consumers playing a greater role in the management of their healthcare through digital health the privacy guidance provided by federal law must also shift to reflect the new reality.

Keywords: HIPAA, digital health, privacy, health data, consumer informatics

Introduction

Throughout history, ethics rather than regulation governed the privacy of patient information. Originally, individuals were concerned primarily with invasion of their homes, financial records and personal conversations yet with the proliferation of digital health tools individuals are becoming more aware of the vulnerability of their health data.[1] The digitization of healthcare coupled with consumers taking a more active role in their healthcare management has created an abundance of health data that falls between the cracks of current privacy regulations.[2] Current regulations have emerged over time; initially rooted in ethical principles and often loosely interpreted and applied to health information.

One of the first attempts to regulate privacy of health information was the Privacy Act of 1974. It focused on protection of health records collected and maintained by the Federal Government. Most notably, only federal agencies were required to comply, although it did give best practices for use

and disclosure of patient information. Healthcare providers were predominantly unaffected and continued to practice privacy based on ethics until more comprehensive legislation was passed.[3]

Previous attempts at privacy regulations were insufficient; therefore, the Health Insurance Portability and Accountability Act of 1996 was written and included the privacy and security rules creating comprehensive yet general restrictions for health information privacy. HIPAA remains the most critical law related to healthcare privacy because it provided a direct and unavoidable right to privacy for all patients.[4–6]

Compliance with the original HIPAA regulations took significant time and effort by healthcare facilities, and more changes were on the horizon as the focus on patient rights grew. As the challenges and risks of healthcare privacy took center stage, legislators became increasingly eager to draft privacy legislation with a narrower scope.

In the late 1990s, discrimination based on genetic information became a major concern for patients and physicians. Genetic data is more sensitive than clinical patient data as it involves identification of not only the individual patient but also his/her family members. Modern courts recognized the sensitive nature of genetic information, and their decisions reflected a perceived need for additional protection of this type of information beyond what HIPAA offered.[7,8] Congress passed the Genetic Information Nondiscrimination Act (GINA) in May of 2008. GINA became the legal standard for the collection, use, and disclosure of genetic information.[7,8] Although only focused on genetic information, GINA served as a further step in the evolution of health information privacy laws.

The American Recovery and Reinvestment Act (ARRA) passed in 2009 intended to provide economic stimulus to the sluggish American economy.[9] The healthcare industry was front and center in many parts of the Act, but mostly in the Heath Information Technology for Clinical Health Act (HITECH) portion.[9] While spotlighting and investing in electronic health records and healthcare information technology, HITECH also amended some privacy provisions of HIPAA. It redefined some key terms found in HIPAA as well as creating an official structure for governance of policy and standards relating to healthcare privacy and security.

HITECH's Meaningful Use program successfully incentivized adoption of Electronic Health Records with substantial increases in use of IT throughout the healthcare industry.[10,11] This moved much of the traditional patient data from a paper record to a digitized format which was encouraged by HITECH. Meaningful Use created new channels of health data access (i.e., patient portals) for patients to access their health information, but it also introduced new concerns for health data privacy.[12] Although HITECH made great advancements in health information technology, it failed to address the new privacy and security challenges presented by the digitization of health information.[13]

Up to this point, the aforementioned privacy and security laws did not address the transition of healthcare into the digital age. With the implementation of digital heath tools such as patient portals, health information exchanges, genomic registries, wearables, and mobile health (mHealth) applications, a void in the protection of health data emerged.

Modern Privacy Laws

Recent attempts have been made at the federal and state level to acknowledge digital health data however privacy and security guidance has been limited. For instance, the 21st Century Cures Act was signed into law (2016) reflecting a major push in the pharmaceutical industry to modernize drug development and create innovative pathways and clinical trials.[14] This legislation did address interoperability issues associated with data exchange and emphasized a patient's right to access their own information, yet it did not go far enough to change or reclassify patient privacy or further define the data that is covered by privacy regulations.[15,16]

Where no federal law or less restrictive federal law exists, states are allowed to pass legislation at their discretion. Given the lack of comprehensive privacy law updates as well as modern advancements in how healthcare data is managed, stored and transmitted, many states have individually passed privacy laws that are stricter than HIPAA, GINA and ARRA. Many of these state laws also deal with digital health data as well as reinforcing patient rights.

For instance, the state of California recently passed a unique privacy law focused on protecting residents' data privacy rights.[17] The California Consumer Privacy Act was signed into law in 2018 with a 2020 compliance date. This legislation addresses modern challenges associated with consumer privacy such as opt-out options for consumers who do not wish for their information to be sold to third parties as well as more detailed disclosure of how consumer data is used to promote transparency and understanding by consumers. The main limitation of CCPA is the narrow scope of businesses that must comply. Primarily this law focuses on large corporations with substantial revenues and/or customer volume.[17]

In 2018, Colorado passed an innovative law requiring the most stringent measures in the United States to protect consumer data privacy. The Colorado Consumer Privacy Act defines a covered entity as any organization or person who "maintains, owns, or licenses personal identifying information of an individual residing in Colorado."[18] This is a much broader definition than HIPAA provided and includes many of the corporations not covered by the HIPAA definition of a covered entity. The Colorado law's breach notification terms include a more stringent timeframe (30 days compared to 60 days in ARRA) as well as requiring notification of Colorado government officials of any breach affecting more than 500 residents.[18] Finally, the data included in this law includes both

healthcare as well as financial data.[18]

Similar to the Colorado Consumer Privacy Act, the European Union (EU) implemented new regulations of digital data privacy to include healthcare data. The EU General Data Protection Regulation passed in 2016 with a compliance date of May 2018, is a notable international law aimed at protecting privacy of individuals in the European Union.[19,20] The legislation mimics HIPAA in some areas with breach notification rules, penalties, and patient rights however it focuses on data, technology, cloud-based applications and third-party access to data.[19,20] Many see this law as an upgrade to the outdated version of HIPAA still used in the United States.[19,20]

Even with these notable changes there are still health data privacy concerns as many digital health tools are not covered by current HIPAA privacy laws. For instance, recent research has shown that some mobile health (mHealth) applications leave residual protected health information data on the hardware of the device utilized.[21,22] This leaves the consumer's health data vulnerable to be utilized or accessed for purposes other than which the consumer agreed upon.[23,24]

Current Challenges with Digital Data and Privacy

Emerging technologies such as genealogical databases (i.e. 23andme and Ancestry) as well as wearable devices and mHealth apps have created a new risk for data privacy that is not covered by HIPAA. These digital health tools are not covered entities therefore they are not required to protect the data they collect under HIPAA. The Department of Health and Human Services nor the Office of Civil Rights have purview over this data or any breach of the consumer's information. Any complaint regarding a breach of consumer's health data is rejected, as there is no controlling law currently for this type of data. Complaints of this type go to the Federal Trade Commission; however, many consumers are never aware that their information is breached, shared or sold to a third party because there is no breach notification requirement in place.

The novel Coronavirus (COVID-19) pandemic has further highlighted the need for the modernization of HIPAA. Although HIPAA disclosure laws found in the Privacy Rule remained applicable for sharing of patient data for patient care and public health purposes, the considerable increase in use of telehealth as a result of COVID-19 poses challenges for HHS. In March 2020, HHS released a notification of enforcement discretion surrounding use of remote communication applications, software and technology such that the use of those technologies is in good faith.[25] This included use of video chat and communication platforms supporting telehealth visits which did not require Business Associate Agreements for these third-party vendors as normally required under HIPAA. The mechanisms of delivery of healthcare have been completely altered, use of technology is now undeniable and applicable laws such as HIPAA must be revised.

Consumer Health Informatics

The field of consumer informatics continues to grow rapidly as consumers (i.e. patients) take a more active role in their healthcare utilizing technology such as: patient portals, online forums, personal health records, wearables, medical Internet of Things (IoT) and mobile health applications (mHealth).

Medical internet of things (mIoT) is a system that connects devices such sensors, smartphones (mobile health apps), wearables, smart TVs and intelligent virtual assistants (i.e. Amazon Echo, Google Home) to facilitate the healthcare delivery process.[26] The assimilation of mIoT and mobile health apps into the healthcare ecosystem has vastly changed the manner in which healthcare is delivered and has the potential to improve the quality, safety and efficiency of healthcare services.[27–29] Medical internet of things (mIoT) is driven by the monitoring of personal health information by sensors and the analyzation of the data received from these sensors. mIoT and mobile health applications have emerged as revolutionizing technologies that are redefining the way patient data is accessed, stored and delivered.

While accessing and utilizing these consumer informatics tools helps consumers make more informed health decisions it also presents a privacy challenge since most of the consumer health informatics tools are not governed under the HIPAA Privacy Rule.[30] This is especially true in the wearables and mHealth app markets where these tools/applications seem to fall between FDA regulation and the HIPAA Privacy Rule.[31] Many wearables and mHealth solutions store consumer health data on the cloud of which the consumer may be unaware.[30] As long as the consumer health informatics tool is not integrated as part of a healthcare system then the consumer health informatics tool vendor does not have to meet HIPAA or HITECH guidelines.[30,32] This leads to a critical gap in privacy protection where consumers have very little understanding and control of how their health data is stored, accessed and utilized.

Genomic Data

With reductions in the cost of genomic sequencing there has been an increase in the utilization of genomic data for clinical research and healthcare delivery.[33] In addition, there are new options such as direct-to-consumer genetic testing which allows consumers to initiate genetic testing for specific mutation risks. For instance, the FDA allowed 23andMe a direct-to-consumer *BRCA1* or *BRCA2* mutations testing for women to help identify breast cancer risks.[34] Due to the gaps in health data privacy across the digital health ecosystem there has been an increase in the sophistication of attacks on stored genomic data.[33] These sophisticated attacks utilize public information (e.g. demographic data and genealogical data), genomic-sharing websites (e.g. PatientsLikeMe), online forums and online social networks to triangulate the data in an effort to identify the consumer (i.e.

patient).[33] Genomic data is another segment of digital health data that that lacks appropriate protection under GINA and HIPAA.

Conclusion

In 1963, Justice Earl Warren was quoted as saying "The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual."[35] This prophetic statement speaks to the challenges faced in health information privacy today.

With no major updates in the last 20 years, HIPAA remains the preeminent comprehensive health information privacy law. HIPAA was written and passed in the late 20th century when the health information environment was primarily paper based and before the explosion of digital health tools. Two decades later, the health information industry has transformed leaving substantial gaps between advancements in digital health and privacy laws. Individual states as well as the European Union have taken more modern approaches to creating privacy laws reflecting contemporary practices thus demonstrating an awareness of the challenges that exist in management of digital data. These modern approaches to legislation could serve as guides for necessary changes to federal law. Although the benefits of digital data and the opportunities associated with electronic data are "fantastic" as proclaimed by Warren, he was also accurate in his prediction of the dangers now challenging the patient's right to privacy.[35] In order to protect consumer health data so that consumers and health professionals can leverage the power of data in the digital age, revisions to the current privacy laws are vital.

Kim Theodos, JD, MS, RHIA, (theodos@ulm.edu) is associate professor of Health Studies at the University of Louisiana Monroe.

Scott Sittig, PhD, MHI, RHIA, (sittig@southalabama.edu) is assistant professor School of Computing, University of South Alabama.

References

1. Xu Z. An empirical study of patients' privacy concerns for health informatics as a service. Technological Forecasting and Social Change. 2019 Jun 1;143:297–306.

2. Glenn T, Monteith S. Privacy in the digital world: medical and health data outside of HIPAA protections. Curr Psychiatry Rep. 2014 Nov;16(11):494.

3. Solove DJ. A Brief History of Information Privacy Law. GW Law Scholarly Commons. 2006;47.

4. Goldstein MM, Pewen WF. The HIPAA Omnibus Rule: Implications for Public Health Policy and Practice. Public Health Rep. 2013;128(6):554–8.

5. Majumder MA, Guerrini CJ. Federal Privacy Protections: Ethical Foundations, Sources of Confusion

in Clinical Medicine, and Controversies in Biomedical Research. AMA Journal of Ethics. 2016 Mar 1;18(3):288–98.

6. Cohen IG, Mello MM. HIPAA and Protecting Health Information in the 21st Century. JAMA. 2018 Jul 17;320(3):231–2.

7. Feldman EA. The Genetic Information Nondiscrimination Act (GINA): Public Policy and Medical Practice in the Age of Personalized Medicine. J Gen Intern Med. 2012 Jun;27(6):743–6.

8. Erwin C. Legal update: living with the Genetic Information Nondiscrimination Act. Genet Med. 2008 Dec;10(12):869–73.

9. Carley S, Hyman M. The American Recovery and Reinvestment Act: Lessons from Energy Program Implementation Efforts. State and Local Government Review. 2014 Jun 1;46(2):130–7.

10. Jha AK. Meaningful Use of Electronic Health Records: The Road Ahead. JAMA. 2010 Oct 20;304(15):1709–10.

11. Slight SP, Berner ES, Galanter W, Huff S, Lambert BL, Lannon C, et al. Meaningful Use of Electronic Health Records: Experiences From the Field and Future Opportunities. JMIR Med Inform . 2015 Sep 18 ;3(3). Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4704893/

12. Kruse CS, Bolton K, Freriks G. The Effect of Patient Portals on Quality Outcomes and Its Implications to Meaningful Use: A Systematic Review. Journal of Medical Internet Research. 2015;17(2):e44.

13. GOLD M, McLAUGHLIN C. Assessing HITECH Implementation and Lessons: 5 Years Later. Milbank Q. 2016 Sep;94(3):654–87.

14. Gabay M. 21st Century Cures Act. Hosp Pharm. 2017 Apr;52(4):264–5.

15. Kesselheim AS, Avorn J. New "21st Century Cures" Legislation: Speed and Ease vs Science. JAMA. 2017 Feb 14;317(6):581–2.

16. Avorn J, Kesselheim AS. The 21st Century Cures Act — Will It Take Us Back in Time? New England Journal of Medicine. 2015 Jun 25;372(26):2473–5.

17. Stephens J. California Consumer Privacy Act . 2019 . Available from: https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/

18. Peters I. HIPAA-Covered Entities: It's Time to Cover Yourself . The National Law Review. 2018 . Available from: https://www.natlawreview.com/article/hipaa-covered-entities-it-s-time-to-cover-yourself

19. Phillips M. International data-sharing norms: from the OECD to the General Data Protection

Regulation (GDPR). Hum Genet. 2018 Aug 1;137(8):575–82.

20. Dove ES. The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. J Law Med Ethics. 2018 Dec 1;46(4):1013–30.

21. Miller S, Glisson W, Campbell M, Sittig S. Risk Analysis of Residual Protected Health Information of Android Telehealth Apps. AMCIS 2019 Proceedings . 2019 Jul 8; Available from: https://aisel.aisnet.org/amcis2019/healthcare_it/healthcare_it/28

22. McGowan A, Sittig S, Menard P. mHealth Cross-Contamination of User Health Data: Android Platform Analysis. AMCIS 2019 Proceedings . 2019 Jul 8; Available from: https://aisel.aisnet.org/amcis2019/healthcare_it/healthcare_it/12

23. Cilliers L. Wearable devices in healthcare: Privacy and information security issues. Health Inf Manag. 2019 May 30;1833358319851684.

24. Hewitt B, Dolezel D, McLeod A. Mobile Device Security: Perspectives of Future Healthcare Workers . . Available from: https://perspectives.ahima.org/mobiledevicesecurityperspectives/

25. Rights (OCR) O for C. Notification of Enforcement Discretion for Telehealth . HHS.gov. 2020 . Available from: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

26. Sadoughi F, Behmanesh A, Sayfouri N. Internet of things in medicine: A systematic mapping study. J Biomed Inform. 2020 Mar;103:103383.

27. Kadhim KT, Alsahlany AM, Wadi SM, Kadhum HT. An Overview of Patient's Health Status Monitoring System Based on Internet of Things (IoT). Wireless Pers Commun. 2020 Oct 1;114(3):2235–62.

28. Shehabat IM, Al-Hussein N. Deploying Internet of Things in Healthcare: Benefits, Requirements, Challenges and Applications. J Commun. 2018;

29. Proceedings of the 5th EAI International Conference on Smart Objects and Technologies for Social Good | ACM Other conferences . . Available from: https://dl.acm.org/doi/proceedings/10.1145/3342428?tocHeading=heading6

30. Perez AJ, Zeadally S. Privacy Issues and Solutions for Consumer Wearables. IT Professional. 2018 Jul;20(4):46–56.

31. Shuren J, Patel B, Gottlieb S. FDA Regulation of Mobile Medical Apps. JAMA. 2018 Jul 24;320(4):337–8.

32. Mitchell M, Kan L. Digital Technology and the Future of Health Systems. Health Systems & Reform. 2019 Apr 3;5(2):113–20.

33. Mohammed Yakubu A, Chen Y-PP. Ensuring privacy and security of genomic data and functionalities. Brief Bioinformatics. 2019 Feb 12;

34. Gill J, Obley AJ, Prasad V. Direct-to-Consumer Genetic Testing: The Implications of the US FDA's First Marketing Authorization for BRCA Mutation Testing. JAMA. 2018 Jun 19;319(23):2377–8.

35. Stone GR. The Scope of the Fourth Amendment: Privacy and the Police Use of Spies, Secret Agents, and Informers. American Bar Foundation Research Journal. 1976;1(4):1193–271.

There are no comments yet.