Bloomberg BNA

BNA's
Health Care Policy Report™

Health Information

Critical Next Steps: Addressing Health Privacy and Security Gaps Identified by ONC



BY JODI DANIEL, ELLIOT GOLDING AND JENNIFER WILLIAMS

Adding to a growing chorus, the Office of the National Coordinator for Health Information Technology (''ONC'') released a report on July 19, 2016, expressing concerns about major gaps in regulating health information privacy and security. This report comes in the midst of an explosion of healthcare technology and emphasizes the importance of safeguarding electronic health data collected by wearable fitness trackers, health social media, and mobile health apps, while maintaining the innovation momentum, fostering a ''predictable business environment,'' and ensuring that individuals have timely and convenient access to their health data.

The ONC report frames the privacy and security problems well and highlights many of the most critical deficiencies, but largely punts to the private sector to develop a solution. This article provides context for the ONC findings and provides several recommendations to address the problems ONC raises. All entities – whether subject to HIPAA or not – should continue to follow this issue closely as the industry and new standards and requirements continue to evolve.

Jodi Daniel is a partner in Crowell & Moring's Health Care Group and is the former policy director in the HHS Office of the National Coordinator for Health Information Technology. Elliot Golding is a counsel in the firm's Privacy & Cybersecurity Group. Jennifer Williams is a Health Care associate.

Legal Background

The United States is one of few countries to use a sector-by-sector approach to data privacy rather than a comprehensive data protection law. The result is a patchwork of laws that protect some health information, but leave large amounts of health information largely unregulated. The Health Insurance Portability and Accountability Act (''HIPAA'') is the primary law that regulates certain health information, but applies only to a limited number of entities – namely Covered Entities (''CE'') (i.e., health plans, health care clearinghouses, and certain health care providers) and Business Associates (''BA'') (i.e., entities that handle health information on behalf of Covered Entities). This limited applicability worked reasonably well for the decade after HIPAA was enacted in 1996 when health information was handled predominantly by CEs and BAs.

Other federal and state laws also regulate health information, but only certain types or only certain practices. For example, federal law protects the confidentiality of substance use disorder information, but only information maintained by certain types of facilities and third parties that obtain the information from such facilities. Many state laws protect the confidentiality of mental health, genetic testing, or HIV/STD information, but such laws also often apply only to certain entities.

 ISSN 1068-1213

The Federal Trade Commission has authority under Section 5 of the Federal Trade Commission Act (and states have authority under similar state laws) to stop companies from engaging in unfair or deceptive practice, such as failing to implement reasonable data security or failing to adhere to posted privacy policies.

These laws, however, leave a large portion of the health care sector essentially unregulated (leaving aside the FTC and state Attorney Generals' power to stop unfair and deceptive trade practices). Worse, the existence of strong protections in HIPAA and other laws often leads consumers to believe that their health information is protected when it is not, and may leave many companies uncertain about which laws apply to them. The rapid increase in consumer-facing health tools over the past decade, which are generally not subject to HIPAA or other state and federal laws governing health information, has reached a tipping point where such gaps can no longer be ignored.

ONC Findings

The ONC report focuses on two main areas that HIPAA and other existing laws generally do not reach: (1) mHealth technology, which refers to products that collect and share health information directly from individuals, such as personal health record (''PHR'') technology, wearable fitness trackers, and other cloud-based or mobile software tools; and (2) health social media, which refers to social media sites through which consumers can share information about their health with others. The ONC report highlights many of the problems regarding the lack of laws or consistent privacy and security standards applicable to such products, such as:

- New types of entities that collect, share, and use health information are not regulated by HIPAA;
- Individuals may have a limited or incorrect understanding of when data about their health is protected by law, and when it is not;
- Health information collected in more places without consistent security standards may pose a cybersecurity threat (of which individuals may be unaware);
- Individuals generally have greater rights regarding access to data held by HIPAA covered entities than data held by non-covered entities; and
- The lack of understanding of what rules apply may hinder economic growth and development of beneficial products that could generate better health, smarter spending, and healthier people.

Some policymakers have taken meaningful steps to fill the gaps in oversight of entities not regulated by HIPAA. For example, the FTC has issued many reports with privacy and security recommendations. The FTC has also undertaken enforcement action against entities that collect health data and have failed to follow their own stated policies. Yet, the FTC's enforcement ability is limited because entities not regulated by HIPAA are not necessarily required to have privacy and security policies in place, there are no baseline requirements, and the FTC does not have the authority to force an entity to follow a non-existent policy.

Leaders in the private sector have also sought to address the lack of clear guidance by promulgating their own standards. In late 2015, for example, the Consumer Technology Association issued a set of voluntary guidelines for wellness data to address tangible privacy risks and consumer preferences. The guidelines include many of the Fair Information Practice Principles that the Department of Health and Human Services has emphasized for over forty years (such as securing data, providing notice to consumers, etc.). These guidelines, however, only apply to limited data (wellness data) and, more importantly, have apparently not been adopted by any company to date. The lack of adoption might be evidence of no economic incentive to adopt these guidelines and no clear mechanism for consumers to know if these guidelines have been met.

What Next?

The ONC report helps identify the problems, but ONC acknowledges that the report is not intended to propose solutions. Rather, ONC urges the private sector and other stakeholders to develop solutions. This requires answering three questions. First, why is developing standards and requirements beneficial? Second, what should those standards and requirements be? Third, how should data holders be held accountable for meeting these standards and requirements?

The first question is more complicated than it sounds. Consumers obviously benefit if their information is more (and more consistently) protected, if they have greater control over the data, and if there is more transparency around data uses and disclosures. But companies can also benefit significantly from developing standards in this space as well. For example, companies often do not know what laws apply to the information they handle, making it difficult to develop innovative approaches for capturing and using information to improve health. More certainty around data privacy requirements would help companies minimize enforcement risk by understanding the limits of what they can do. Companies would also benefit if consumers were less confused about data privacy and security. Consumers may wrongly believe their data is subject to HIPAA (and become upset when it is handled inconsistently with HIPAA's protections) or may be too wary about the lack of protections to participate at all with new technologies. Either way, more certainty would again have benefits for mHealth, remote monitoring tools, and health social media companies.

The second question about standards really has two components: (a) who should develop the standards, and (b) what should they be. Any standards must appropriately balance maintaining the innovation momentum, fostering a ''predictable business environment,'' and ensuring that patients have timely and convenient access to their health data. An industry-led effort would likely be preferable to accomplish these goals because industry is in a better position to understand the business needs. An industry-led effort would also likely provide more flexibility as technology continues to evolve than a government-led effort, which often takes a long time to modify in response to such changes.

In terms of what standards to implement, it is important to build on existing frameworks for privacy and se-

  HCPR ISSN 1068-1213

curity protections, such as Fair Information Practice Principles, ensure compatibility with HIPAA, and consider expectations of various parties including consumers and health care providers. It is also important to consider how rules regarding health information uses and disclosures may limit the usefulness of the service being offered or impact business models in such a way that innovation is stifled. Finally, it is important to consider new technological capabilities to protect data or to provide consumers more control as well as how technological innovation may cause increased risks to privacy and security. The best way to address these challenging questions is to convene diverse private stakeholders that can work through these issues.

Third, there needs to be a mechanism for holding health data holders accountable for meeting the standards and requirements. This can be done through legislation and regulation; however, it is difficult for the government to act in this space, as evidenced by the six-year delay in the release of this report. Furthermore, given the FTC's enforcement of policy statements, it may be equally, if not more effective to have the private sector develop an accreditation program or a seal of approval. Health data holders could then use such a system to demonstrate compliance with privately developed standards to regulators and consumers, and make representations that, if not met, could be enforced by FTC's existing authority.

This convening is an important next step and could reduce the gaps in protections and the resulting problems identified in ONC's report.