DrinkerBiddle

Client Alert

July 28, 2016

New HHS Report Identifies Privacy and Security Gaps in Emerging Technologies

By Peter A. Blenkinsop and Reed Abrahamson

Key Takeaways:

- The HHS Report highlights gaps in consumer privacy and security protections outside the traditional health care environment but does not outline specific recommendations.
- While HHS specifically notes that existing laws and regulations have not kept pace with new technologies, the Department appears primarily focused on stakeholder engagement and private sector efforts rather than seeking new legislative authority.

On Tuesday, July 17, 2016, the Office of the National Coordinator for Health Information Technology (ONC) issued a report titled, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA*. The report, required under the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, highlights the lack of clear policy guidance around consumer access, privacy, and security when it comes to relatively new technologies that allow individuals to monitor their personal health. When Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996, products such as fitness trackers and social media sites did not exist. As a result, these non-covered entities (NCEs) may collect, share, and use consumer health data without oversight under HIPAA regulations.

The report focused on two types of new products that are generally NCEs: mHealth technologies and health social media. The first, mHealth technologies, includes entities that collect or deal in personal health records as well as mobile software tools (such as fitness trackers) that collect health information from individuals directly. The second, health social media, captures websites where individuals share information on their health conditions. The report did not cover products where health information is derived from other data, casual disclosures on social media sites like Facebook or Twitter, or products that may meet the definition of a medical device under section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C).

Five Gaps in the Existing Regulatory Oversight

In its report, ONC examined the existing regulatory and oversight structure for health information, which includes HIPAA's privacy, security, and breach notification protections, Section 5 of the Federal Trade Commission Act, and the FTC Health Breach Notification Rule. It identified five major areas where the security oversight of NCEs differs from HIPAA protections:

- **Individuals' Access Rights.** Users do not have the same rights when they provide information to NCEs as they would have under HIPAA, including to access information about themselves, the ability to demand an accounting of certain disclosures, and the ability to control how the information is used and shared.
- **Re-Use of Data by Third Parties.** Data collectors are not required to protect users against unwanted marketing. Though the FTC can require reasonable data security protections, absent a specific showing of deception or unfairness, it cannot prohibit downstream use by marketers or mandate providing consumers with access to their information.
- **Security Standards Applicable to Data Holders and Users.** Minimum regulatory standards do not exist for encryption, identity verification, and identity authentication where health information is stored. NCEs operated by vendors may lack consistent risk assessment and audit capabilities.
- **Terminology About Privacy and Security Protections.** Federal requirements for policies and notices informing individuals about privacy and security practices do not apply to NCEs. Where privacy policies do exist, they may be difficult to locate and understand, and product developers may not consistently use key terms like "individually identifiable health information" to mean the same thing. NCEs can also modify privacy policies without notice.

- **Inadequate Collection, Use, and Disclosure Requirements.** NCEs are not required to collect only the minimum information necessary to accomplish a specified purpose. They can freely engage in online advertising and marketing, sale of an individual's information, and behavioral tracking practices.

Next Steps

The report proposed that the five oversight gaps should be filled, though it did not outline specific recommendations. It drew attention to certain ongoing efforts, including FTC's policy and informational initiatives, and private sector efforts to fill the gaps through published codes of conduct. A blog post jointly released by ONC and OCR indicates that the report is only a first step and will be followed by engagement with stakeholders on how to address the gaps in order to ensure consumers' privacy, security, and access to health data, while fostering a predictable business environment.

Notably, although the ONC spoke generally about the FTC's authority under Section 5, the ONC did not discuss recent guidance from the FTC on privacy and data security requirements for businesses. Although the FTC's June 2015 "Start with Security" guidance describes the FTC's past enforcement actions on issues like encryption of sensitive personal information, authentication requirements, vendor assessments, and routine network monitoring, a casual reader of the ONC's report could be forgiven for assuming that the FTC has not articulated standards or taken enforcement action. The FTC's authority to regulate data privacy and security matters survived a direct challenge in the Wyndham Hotels case before the Third Circuit last August, and NCEs should take care to examine the FTC's past settlements and enforcement patterns before concluding that no existing data security standards apply to their products.

Information Privacy, Security and Governance Team

Primary Contacts

Peter A. Blenkinsop
Partner
Washington
(202) 230-5142
Peter.Blenkinsop@dbr.com

Reed Abrahamson
Associate
Washington
(202) 230-5672
Reed.Abrahamson@dbr.com