HHS Report Highlights Security Gaps in Entities not Protected by HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) has been around since 1996. And while that might not seem like an especially long stretch of time, it's practically an epoch when one considers how fast technology has changed, and how thoroughly technology shapes daily life.

Where that's most relevant to HIPAA: social media sites were not in existence when Congress enacted HIPAA in the mid-'90s, and yet now they arguably dominate interpersonal dynamics. But what this means in terms of HIPAA is that non-covered entities (NCEs) like social media sites or fitness trackers are not bound by HIPAA regulations and can—without federal oversight—collect, share, and use consumer health data.

"Without oversight" does not imply a permanent state, though. Or at least not one that's exempt from analysis. On July 17th, 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 centers around two kinds of NCEs: health social media and mHealth technologies. The former captures websites where people are sharing details about their medical conditions. The latter involves mobile software tools (like personal fitness trackers) where individuals directly transmit their health information. However, the report does not address casual health disclosures on sites like Twitter or Facebook, products that fulfill the criteria of a medical device under section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C), or sites or software that gather health information from other data.

Report identifies troubling gaps in privacy and security oversight of NCEs

The ONC report looks at the current structure of regulations for health information, including HIPAA's privacy, security, and breach notification safety measures, the Federal Trade Commission (FTC) Health Breach Notification Rule, and Section 5 of the FTC Act. While the report acknowledges the "extraordinary pace" of technological change since HIPAA's creation, it zeroes in on areas of the most concern when it comes to safeguarding sensitive health information, areas where "privacy and security protections of health information have not kept up." Most specifically, the areas where security offered by HIPAA entities and NCE entities diverge, leaving gaps in protection:

- **Difference in Individuals' Access Rights.** The report notes that NCEs often "lack transparency," since they are not bound by statutes or regulations as HIPAA entities are. The example given is of an individual sharing information about his/her health through health social media or an mHealth technology, but later being unable to discover where and how that information was re-disclosed. Ultimately, outside of HIPAA, "there is no legal right to access one's health data."

- **Differences in Re-Use of Data by Third Parties.** HIPAA stipulations limit and regulate the instances of a covered entity sharing protected health information (PHI). In that way, the amount of sensitive health information in the hands of ungoverned third parties is limited. But individuals that share health information with NCEs are not offered that same level of protection. The report gives the example of how this would play out in terms of marketing. HIPAA regulations limit the use of PHI for marketing. NCEs are not bound by this, so if the data collector is an NCE and does not promise to protect the PHI, the information is likely to be used for marketing purposes.

- **Differences in Security Standards Applicable to Data Holders and Users.** The ONC report also found major differences between HIPAA-covered entities and NCEs in terms of security measures, specifically: lack of encryption of sensitive data; inadequate safeguarding of health information via means other than encryption; and a misunderstanding of security risk assessment and audit capabilities. (Because NCEs do not operate under uniform guidelines as HIPAA-covered entities do, the report notes the possibility of NCEs lacking "consistent and appropriately defined" guidelines for assessing risks and conducting audits.)

- **Differences in Understanding of Terminology About Privacy and Security Protections.** Unlike HIPAA entities, there are no federal regulations that mandate NCEs to inform individuals about activities that may compromise the privacy and security of their PHI. Although no nationwide standard exists for NCEs, some states have adopted their own regulations. However, many states have not, which obviously results in a high level of inconsistency across the board. When NCEs do include privacy policies, the report notes that they may be difficult to locate and to read. This point underscores the ONC's criticism of NCEs as often lacking openness and transparency.

- **Inadequate Collection, Use, and Disclosure Limitations.** The report highlights this concern regarding the collection and use of PHI: "Advertising practices and third-party personal data collection may lack limitations on information sharing or use of information for marketing." Individuals that share health information online may not expect that that same information might be sold to a third-party for marketing, or that it may be used for "behavioral tracking practices," but the reality is that with an NCE, it is a distinct possibility.

Because the ONC report does not include suggestions for how these five gaps are to be filled, it seems that the report's main purpose is to draw awareness to the gaps themselves. Clearly what will not change is society's engagement with social media and the like. As the report notes: "Nearly every aspect of the modern citizen's life has a virtual or electronic component."

But it goes on to warn: "…as the electronic sharing and storage of health information increases, and as individuals become more engaged in sharing personal health information online, organizations that are not regulated by HIPAA, the FTC, or state law may collect, share, or use health information about individuals in ways that may put such data at risk of being shared improperly."

For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.