Issue Brief

Extending the HIPAA Individual Right of Access to Non-Covered Entities (NCEs)

Problem

For more than twenty years, Congress has prioritized individuals' access to their health information as a key means to improve care, enable research, and empower Americans to live healthy lifestyles. However, from the paper-based world of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to the digital aspirations of the 21st Century Cures Act (Cures), the ability of individuals to access and use their health information continues to be a challenge. This challenge has only compounded in recent years, with the proliferation of mobile health (mHealth) and health social media applications, which are typically not covered by HIPAA's right of access. Such technologies are examples of HIPAA "Non-Covered Entities" (HIPAA NCEs). While Congress has passed several policies and the U.S. Department of Health and Human Services (HHS) has implemented a host of programs to improve patient data access, patients find that they have little access to and/or control of their health information collected by most HIPAA NCEs.

Background: Non-Covered Entities

Except in certain circumstances, the HIPAA Privacy Rule[1] guarantees individuals the right to review and obtain a copy of their protected health information (PHI) in a covered entity's designated record set. The designated record set includes records maintained by or for a covered entity that are used to make decisions about individuals; a covered provider's medical and billing records about individuals; or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.

A 2016 report from the Office of the National Coordinator for Health Information Technology (ONC) found there are many health-related technologies that exist and operate outside of the scope of HIPAA.[2] While these health-related technologies produce and manage individually identifiable health information, they are not bound by or required to abide by rules established under HIPAA because they are not considered "covered entities" or "business associates." The report further explains that while some HIPAA NCEs may be regulated by the Federal Trade Commission (FTC) and/or state laws, other health-related applications that deal with or manage consumer health data may not fall under any regulatory authority at the federal or state level. Rather, it may be left to the discretion of the health application itself as to whether such information may be shared with the individual. Moreover, FTC and most state laws are concerned with security protocols, focusing their attention on the most egregious breaches and lax security protocols. This kind of oversight does not provide the same type or level of protections for consumers as HIPAA, which offers such safeguards as breach notification; restrictions on the sale, use, and reuse of PHI by third parties; and the individual right of access.

According to a 2018 Accenture survey, 75 percent of consumers said technology is important to managing their health.[3] The research also showed increased usage of mobile apps, electronic health records, social media, wearables, and online communities.[4] Nearly half (48 percent) of healthcare consumers reported using mHealth apps, compared to just 16 percent in 2014.[5] These technologies collect PHI, but in most cases are not subject to HIPAA. Consumers are often not aware that they have no legal right to nor control of data collected by a HIPAA NCE.

Recommendations for Extending the HIPAA Individual Right of Access to Non-Covered Entities

Currently, there is no standard definition for HIPAA NCEs, and there exists wide discrepancies in how such entities produce, manage, and share personal health data.

AMIA and AHIMA recommend that lawmakers develop or direct HHS to define HIPAA NCEs in law and at minimum extend HIPAA's right of access to such NCEs. The goal of such a policy is to create a uniform data access policy for individuals using technology developed by an entity that produces and/or manages their individually identifiable health information, regardless of commercial or legal status.

Congress can draw from important work developed by HHS to distill a standard definition for HIPAA NCEs.[2,6] In addition, ONC has developed a model privacy notice designed to help health technology developers provide clear notice to consumers about what happens to their digital health data when the consumer uses a developer's product.[7]

As the lines between consumer and medical information systems continue to blur, Congress must ensure that rights endowed by HIPAA to patients inside the hospital and within the physician's office also apply beyond the clinical setting.

References

[1] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.
[2] https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.
[3] https://www.accenture.com/us-en/insight-new-2018-consumer-survey-digital-health.
[4] Ibid.
[5] Ibid.
[6] https://www.healthit.gov/sites/default/files/maximus_report_012816.pdf.
[7] https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf.