Published on *The National Law Review* https://natlawreview.com

Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health (HIPAA/HITECH) Compliance Strategies for Medical Device Manufacturers

Article By:

Food and Drug Law Group

As computing power continues to become cheaper and more powerful, medical devices are increasingly capable of handling larger and larger sets of data. This provides the ability to log ever expanding amounts of information about medical device use and patient health. Whereas once the data that could be obtained from a therapeutic or diagnostic device would be limited to time and error codes, medical devices now have the potential to store personal patient health information. Interoperability between medical devices and electronic health record systems only increases the potential for medical devices to store personal information.

The concern has become so significant that the U.S. Food and Drug Administration recently issued a draft guidance and letter to industry noting concerns associated with theft or loss of medical information by cybersecurity vulnerable devices. For a more detailed discussion of this issue, see last month's blog post.

This raises another important issue for medical device manufacturers and health care providers: medical device compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Compliance with HIPAA and HITECH has become a major concern for hospitals and health care providers, and will increasingly be an issue that medical device manufacturers will need to deal with.

A medical device manufacturer needs to answer three questions in order to determine whether the collection of patient information by a medical device is subject to HIPAA and HITECH:

- Does the information qualify as Protected Health Information?
- Is a Covered Entity involved?
- Does a Business Associate relationship exist with a Covered Entity?

Protected Health Information

Protected Health Information (PHI) is individually identifiable health information transmitted or maintained in any form or medium.[1] Special treatment is given to electronic PHI, which is subject to both the HIPAA Privacy Rule, and the Security Rule (which only applies to electronic PHI). To be "individually identifiable," the PHI must either identify the individual outright, or there must be a reasonable basis to believe that the information can be used to identify the individual.[2]

"Health information" is any information (including genetic information) that is oral or recorded in any form or medium, and meets two conditions.[3] First, the information must be created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse.[4] Second, the information must relate to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual.[5]

If data collected by a medical device does not meet the definition of "individually identifiable," or "health information," it is not covered under HIPAA and HITECH. For example, a medical device that logs detailed medical diagnostic information about a patient, but includes no means by which that information may be traced to the patient, the data would likely fall outside of HIPAA and HITECH. Alternatively, a medical device, such as a mobile medical app, may request that a user provide detailed medical information about himself or herself. Provided that information is requested outside of the context of a health care provider, health plan, public health authority, employer, life insurer, school or university, HIPAA and HITECH similarly would likely not apply.

Covered Entities and Business Associates

There are two types of persons regulated by HIPAA and HITECH: "Covered Entities" and "Business Associates." A Covered Entity is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a covered transaction.[6] A Business Associate is a person who either creates, receives, maintains, or transmits PHI for a regulated activity on behalf of a covered entity, or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to a covered entity, where the service involves the disclosure of PHI.[7]

Therefore, at a minimum, in order to be subject to HIPAA and HITECH a Covered Entity needs to be involved. For example, medical devices sold directly to consumers for personal use would generally not be subject to HIPAA and HITECH.

Conversely, just because a medical device manufacturer is not a "Covered Entity," HIPAA and HITECH may apply through a Business Associate relationship. Business Associates include Health Information Organizations, E-prescribing Gateways, and others that provide data transmission services with respect to PHI to a covered entity, and that require access on a routine basis to PHI.[8] Business Associates also include persons that offer PHI to others on the behalf of a covered entity, or that subcontract with a Business Associate to create, receive, maintain, or transmit PHI.[9]

---

[1] 45 C.F.R. § 160.103 "*Protected health information*".

[2] 45 C.F.R. § 160.103 "*Individually identifiable health information*" (2)(i) and (ii).

[3] 45 C.F.R. § 160.103 “*Health information*”.

[4] 45 C.F.R. § 160.103 “*Health information*” (1).

[5] 45 C.F.R. § 160.103 “*Health information*” (2).

[6] 45 C.F.R. § 160.103 “*Covered entity*”.

[7] 45 C.F.R. § 160.103 “*Business associate*” (1).

[8] 45 C.F.R. § 160.103 “*Business associate*” (3)(i).

[9] 45 C.F.R. § 160.103 “*Business associate*” (3)(ii) and (iii).

Copyright © 2025, Sheppard Mullin Richter & Hampton LLP.

National Law Review, Volume III, Number 232

Source URL:https://natlawreview.com/article/health-insurance-portability-and-accountability-acthealth-information-technology