Articles + Publications | August 5, 2024

HIPAA Data Management Requirements for Electronic Protected Health Information

Privacy & Cybersecurity Newsletter

WRITTEN BY

Laura L. Ferguson | Emma Bennett

RELATED OFFICES

Houston

While all companies must take measures to safeguard the privacy and integrity of their electronic data, covered entities and their business associates subject to the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") must take specialized care to comply with HIPAA's data management rules found in the HIPAA Privacy and Security Rules. On April 30, 2024, the U.S. Department of Health and Human Services ("HHS") published its HIPAA enforcement highlights, which compiles the five issues most often alleged in HIPAA complaints.[1] Four of the five issues are related to data management: (1) impermissible uses and disclosures of protected health information; (2) lack of safeguards of protected health information; (3) lack of administrative safeguards of electronic protected health information, such as a risk analysis; and (4) use or disclosure of more than the minimum necessary protected health information.[2] This article provides a brief refresh on data management related to electronic protected health information ("EPHI"), from data collection and use to storage and disposal.

Covered entities and business associates must implement administrative, physical, and technical safeguards in compliance with the HIPAA Privacy Rule and HIPAA Security Rule.[3] While the HIPAA Privacy Rule is more prescriptive in this regard and applies to all PHI, including EPHI, the HIPAA Security Rule's approach to data management for EPHI is "flexible," allowing covered entities and business associates to take into consideration (i) the entity's size, complexity, and capabilities, (ii) the entity's technical infrastructure, hardware, and software security capabilities, (iii) the costs of security measures, and (iv) the probability and criticality of potential risks to EPHI when implementing data management practices.[4]

Collection and Use

From a data management perspective at the beginning of the data life cycle, the HIPAA Privacy Rule applies to the collection and permissible uses of EPHI. Where possible (likely not in a treatment scenario), covered entities and business associates should consider minimizing what is collected to reduce risk. Once collected, the overarching rule in HIPAA is that PHI can only be used for treatment, payment, or operations purposes, unless otherwise specified in HIPAA (such as required by law) or with authorization of the individual. Covered entities and business associates should have policies and procedures outlining what the entity can and cannot do with EPHI.

Another rule to remember is the "minimum necessary" standard – this means that when using EPHI for uses other than treatment, a covered entity or business associate must make reasonable efforts to limit the use of EPHI to the "minimum necessary to accomplish the intended purpose of the use, disclosure, or request,"[5] unless an exception applies. Some exceptions to the "minimum necessary" standard include disclosures or requests by a health care provider for treatment, to the individual as permitted in the Privacy Rule, and as required by law.[6]

Storage

Once EPHI is collected, it must be stored in a secure fashion in accordance with the HIPAA Security Rule. The HIPAA Security Rule may be "flexible," but it is certainly not brief when detailing administrative, physical, and technical safeguards for EPHI storage. Administrative safeguards include security management processes, assigning security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency plans, and evaluations. Physical safeguards include facility access controls, workstation use, workstation security, and device and media controls. Technical safeguards include access control, audit controls, measures to safeguard integrity, authentication, and secure transmission procedures. Some safeguards are "addressable" but not required. However, the entity must have a sound reason for electing not to use an addressable safeguard.

The security standards are summarized in an appendix table to Part 164 and is a good place to start when evaluating HIPAA compliance or building EPHI data management systems from the ground up.[7] In addition, the Office of the National Coordinator for Health Information Technology, in collaboration with HHS developed the Security Risk Assessment Tool, which may be helpful for small and medium health care providers to determine compliance with the HIPAA Security Rule.[8]

Destruction

Destruction is the final step in the data lifecycle. While destroying EPHI is not as straightforward as shredding a document, the goal remains the same: render the data unusable, unreadable, or indecipherable. Given the nature of EPHI, the protected information may need to be destroyed in its virtual form or in the physical device where it is stored. For example, a covered entity or a business associate can use a clearing software to overwrite EPHI, removing the EPHI from a physical storage device to reuse the storage device for another purpose, or physically incinerate or pulverize the data storage device entirely.

With data (mis)management leading HIPAA complaints, updating and enforcing administrative, physical, and technical safeguards for EPHI should be at the top of the "risk management" list for covered entities and business associates this summer.

—

[1] HHS is required to investigate all complaints, which may start as an informal call for additional information or turn into a more extensive compliance audit/investigation.

[2] The fifth issue most often alleged in complaints was lack of patient access to their protected health information. See https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (website accessed on June 26, 2024).

[3] See 45 C.F.R. §§ 164.306 (security standards, general rules), 164.308 (administrative safeguards), and 164.310 (physical safeguards), and 164.312 (technical safeguards). In addition, 45 C.F.R. §§ 164.314 (organizational requirements) and 164.316 (policies and procedures and documentation requirements).

[4] Some HIPAA Security Rule implementation specifications are required, and others are “addressable.” If an addressable specification is not reasonable and appropriate to implement, the covered entity or business associate must document why it would not be reasonable and appropriate to implement and instead, implement an equivalent alternative measure where reasonable and appropriate.

[5] See 45 C.F.R. § 164.502(b)(1). ?

[6] See 45 C.F.R. § 164.502(b)(2). ?

[7] ?See 45 C.F.R. § 164?, Appendix A to Subpart C—Security Standards: Matrix.

[8] See https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool (website accessed on June 26, 2024).

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber