Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Encrypt Your Devices or Face HIPAA Penalties

Insight — 11/07/2019

This week, the Office for Civil Rights ("OCR") announced a $3,000,000 HIPAA settlement arising from a medical center's loss of an unencrypted laptop and flash drive. (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/urmc/index.html). This is simply the latest of many HIPAA settlements based on the failure to encrypt mobile devices. Similar settlements have arisen from lost or stolen smartphones, computers, hard drives, or other electronic media that were not properly encrypted.

Encryption is an addressable standard under the HIPAA Security Rule, which generally requires covered entities and business associates to "[i]mplement a mechanism to encrypt and decrypt electronic protected health information" and, for such data transmitted over a network, to "[i]mplement a mechanism to encrypt electronic protected health information whenever deemed appropriate." (45 CFR § 164.312(a)(2)(iv) and (e)(2)(ii)). The OCR explained the standard in a FAQ:

> **Is the use of encryption mandatory in the Security Rule?**
>
> Answer: No. The final Security Rule made the use of encryption an addressable implementation specification. See 45 CFR § 164.312(a)(2)(iv) and (e)(2)(ii). The encryption implementation specification is addressable, and must therefore be implemented if, after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity and availability of e-PHI. If the entity decides that the addressable implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate. If the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure and document the rationale for this decision.

(https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html). Although encryption is not mandatory, it would be difficult to identify an "equivalent alternative measure" of protection so as to satisfy the addressable standard.

Proper encryption allows covered entities and business associates to avoid HIPAA breach reports if the data or device is lost or stolen. The Breach Notification Rule only applies to the breach of "unsecured protected health

information." (45 CFR § 164.404(a)).

> *Unsecured protected health information* means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under [the HITECH Act].

(45 CFR § 164.402). Encryption which satisfies HIPAA standards is not "unsecured"; accordingly, its loss does not require a breach report. (78 FR 5639 and 5644; 74 FR 42741-42, 42765). According to the OCR:

> Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.
>
> - Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
> - Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

(https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html; *see also* 74 FR 42742-43).

On the other hand, HHS commentary makes it clear that the loss or theft of an unencrypted device containing protected health information presumptively requires a breach report. (*See, e.g.*, 78 FR 5671). For example, in its Breach Notification Rule commentary, HHS noted

> the most frequent form of data loss is the result of lost or stolen laptops and data bearing media such as hard drives. If the data on these devices is encrypted, then under the [Breach Notification Rule] definition of a breach, the event would not require the covered entity or the business associate to notify affected individuals.

(74 FR 42765). On the other hand,

> If laptops containing the unsecured protected health information of more than 500 residents of a particular city were stolen from a covered entity, notification under this section should be provided to prominent media outlets serving that city [in addition to individuals and HHS].

(*Id.* at 42752). Significantly, "if a computer is lost or stolen, [HHS does] not consider it reasonable to delay breach notification based on the hope that the computer will be recovered." (*Id.* at 42745). Moreover, the failure to timely report the theft or loss of the unencrypted device would likely constitute "willful neglect", resulting in mandatory HIPAA penalties ranging from $11,182 to $57,051 per individual whose information was on the laptop. (45 CFR §§ 102 and 160.404(a)). In its commentary to the Enforcement Rule, HHS gave the following example of "willful neglect":

> A covered entity's employee lost an unencrypted laptop that contained unsecured protected health information. HHS's investigation reveals the covered entity feared its reputation would be harmed if information about the incident became public and, therefore, decided not to provide notification as required by § 164.400 et seq.

(75 FR 40879).

HHS and the OCR provide numerous resources to assist covered entities and business associates in properly encrypting data, *e.g.*,

- https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html;
- https://www.hhs.gov/sites/default/files/nist800111.pdf;
- https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html;
- https://www.healthit.gov/topic/privacy-security-and-hipaa/how-can-you-protect-and-secure-health-information-when-using-mobile-device;
- https://www.healthit.gov/topic/privacy-security-and-hipaa/how-can-you-protect-and-secure-health-information-when-using-mobile-device/2-install-and-enable-encryption.

Given the rules, guidance, and reported settlements, OCR Director Serverino's warning in the latest press release must be taken seriously:

> Because theft and loss are constant threats, failing to encrypt mobile devices needlessly puts patient health information at risk… When covered entities are warned of their deficiencies, but fail to fix the problem, they will be held fully responsible for their neglect.

(https://www.hhs.gov/hipaa/for-professionals/compliance-

enforcement/agreements/urmc/index.html).

For questions regarding this update, please contact:
Kim C. Stanger
Holland & Hart, 800 W Main Street, Suite 1750, Boise, ID 83702
email: kcstanger@hollandhart.com, phone: 208-383-3913

This publication is designed to provide general information on pertinent legal topics. The statements made are provided for educational purposes only. They do not constitute legal or financial advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the author(s). This publication is not intended to create an attorney-client relationship between you and Holland & Hart LLP. Substantive changes in the law subsequent to the date of this publication might affect the analysis or commentary. Similarly, the analysis may differ depending on the jurisdiction or circumstances. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.