Health Information Compliance Alert

SECURITY: New Security Rule Crackdown Could Strike You

Hospital lands audit number one. Is your facility next?

A low-key approach to keeping tabs on your protected health information (PHI) may leave you with a costly compliance headache.

New development: In March, the **HHS Office of Inspector General** made its first move to audit a health care provider for compliance with the HIPAA security rule, which regulates PHI stored or transmitted electronically. The OIG's first provider target is **Piedmont Hospital** in Atlanta.

"This is the government's first systematic hands-on examination of compliance with any HIPAA regulation," says **Rebecca Williams**, attorney and partner with **Davis Wright & Tremaine** in Seattle, WA.

Background: The **HHS Office for Civil Rights** enforces the privacy rule of the Health Insurance Portability and Accountability Act--and has been doing so for several years.

The agency acts primarily on complaints, however, and then either helps cooperative covered entities correct their violations or refers egregious cases to the **Department of Justice** for potential criminal prosecution. The **Centers for Medicare & Medicaid Services** enforces the security regulation, which until now hasn't been routinely enforced.

Identify Your Vulnerabilities

Providers transmitting PHI from laptops and other mobile devices should be especially vigilant about complying with a related guidance released late last year, the "HIPAA Security Guidance for Remote Use of and Access to Electronic Protected Health Information."

The guidance addresses a variety of mobile devices, notes Williams. Besides laptops, these include home-based personal computers, personal digital systems or PDAs, smart phones, public work stations, wireless access points, USB flash drives, memory cards, floppy disks, CDs, DVDs, back-up media, e-mail, and smart cards.

3 red flags: HHS highlights three key areas of concern for remote use of and access to electronic protected health information, Williams tells **Eli:** access, storage, and transmission.

"Everyone affected should be looking over this document carefully," says Williams.

Required reading: Though the document is called a "guidance," it carries more weight than other documents in the same category.

In issuing the document, the HHS emphasized that the feds "may rely upon this guidance document in determining whether or not the actions of a covered entity are reasonable and appropriate for safeguarding the confidentiality, integrity and availability of [electronic PHI], and it may be given deference in any administrative hearing" under the HIPAA enforcement rule.

Get Cracking on Protection Strategies

Providers can employ a number of tactics to protect electronic PHI, according to experts familiar with the guidance.

CPT® 2023 American Medical Association. All rights reserved.

In addition to locking down laptops and encryption, providers should consider investing in flash drives. Flash drives prohibit staff from putting PHI on laptops or other hard drives, advises **Michael Roach**, partner with **Meade Roache Consulting** in Chicago. Password-protected flash drives are the way to go, he advises.

Caveat: Policies and procedures, no matter how well designed, will not be effective unless the workforce receives appropriate training, reminds Williams.

The bottom line: As CMS itself admonishes in the guidance: "Affected covered entities capable of implementing all of the [recommended] strategies . . . are strongly encouraged to do so."

Resource: To access the guidance, go to www.cms.hhs.gov/SecurityStandard/.

CPT® 2023 American Medical Association. All rights reserved.