"HIPAA wake-up call"

Rick L. Hindmand | Monday, October 8, 2018

Physician practices, like other HIPAA-covered entities, face a daunting array of threats to their patient protected health information (PHI) and must be diligent when protecting the privacy and security of their records.

Reviewing reported breaches can offer healthcare providers, health plans and business associates guidance on how they can protect PHI.

Data breach landscape

Healthcare breaches have become so widespread and difficult to prevent that everyone involved in handling patient information needs to be aware of the importance of the steps that help prevent a breach.

Combining data from the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) reports since mandatory reporting began in 2009 with unresolved breaches in the past 24 months shows the total number of reported incidents through May 2018 exceeds 2,299, affecting almost 262 million individuals.

Insurers (tallied under “Health plan” in Figure 1) were responsible for the highest number of reported breaches, followed by healthcare providers, business associates and lastly healthcare clearinghouses, which process medical claims.

The types of breaches affecting the most individuals over the past eight years have been hacking/IT

incidents (more than 216 million individuals affected) and theft (more than 25.3 million individuals affected). The simplest solution to prevent the hackers from reading or otherwise using the data is by enforcing data encryption that is in accordance with the HHS guidance. Though an objective assessment of a breach incident is always required to determine notification, keep in mind that under the modified HITECH Act of 2009, the loss or theft of a device need not be reported if it was encrypted following the guidance of the National Institute of Standards in Technology (NIST).

Where do you stand on HIPAA?

In its HIPAA settlements and guidance, OCR has focused on the following failures by a covered entity or business associate:

Failure to conduct adequate risk analysis. Risk analysis has been central to most of OCR's published resolution agreements. The HIPAA Security Rule requires each covered entity or business associate to conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by the covered entity or business associate.

In addition to violating the Security Rule on its own, failure to conduct appropriate and timely risk analysis often prevents a covered entity or business associate from taking appropriate risk management steps to protect ePHI, thereby increasing exposure to breaches as well as potential penalties and litigation.

Failure to enter into appropriate business associate agreements (BAAs) before allowing business associates to access PHI. OCR has expanded its enforcement focus on business associates, with a string of resolution agreements holding covered entities accountable for allowing business associates to access PHI without entering into BAAs. OCR specifically reminded covered entities and business associates in October 2017 that using a cloud service provider to maintain ePHI without entering into a BAA violates HIPAA rules and that cloud service arrangements need to be accounted for in risk analysis and risk management. Within the past several years, three physician practices have made settlement payments for disclosing PHI to business associates without BAAs, including a $750,000 payment in 2016 by a North Carolina orthopedic clinic.

Click the link below to access a PDF of the full article by Rick Hindmand and co-authors Andrea Driscoll from AD Healthcare Consulting LLC and Helen Simmons from Medic Management Group LLC.

Read the full article

Rick L. Hindmand