Codify
BY AAPC

Health Information Compliance Alert

Case Study: Learn These Lessons From The Biggest HIPAA Settlement To-Date

Entities agree to pay out a benchmark-setting $4.8 million.

If your company shares a data network and/or has a joint compliance agreement with another healthcare provider, a breach could mean double-trouble and much bigger fines. Here's what you can learn from the costly mistakes involved in this recent breach.

Background: Providers **New York and Presbyterian Hospital** (NYP) and Columbia University (CU) have a joint arrangement in which CU faculty members serve as attending physicians at NYP. The providers also operate a shared data network and firewall, which links to NYP's patient information systems containing electronic protected health information (ePHI), according to a May 7 announcement by the **HHS Office for Civil Rights** (OCR).

A breach occurred when a CU physician who developed applications for both providers attempted to deactivate a personally owned computer server on the network containing NYP patients' ePHI. This allowed the ePHI to become accessible on internet search engines.

After receiving a complaint from an individual who found the ePHI of a deceased partner (who was an NYP patient) on the internet, NYP and CU submitted a joint breach report, OCR states. The report revealed the disclosure of 6,800 individuals' ePHI, including patient status, vital signs, medications, and laboratory results.

Lesson #1: Joint Breach Could Equal Larger Penalties

For the breach, OCR slapped the providers with an astounding $4.8 million in monetary payments $3.3 million for NYP and $1.5 million for CU. As part of the settlement agreement, both providers have also agreed to substantive corrective action plans (CAPs), according to the OCR announcement.

Significance: "In addition to being the largest HIPAA settlement to date, this is the first settlement involving multiple covered entities," noted Tampa, FL-based healthcare attorney **Elizabeth Hodge** in a posting for **Akerman LLP**'s Health Law Rx Blog.

"This settlement is another reminder of the importance that OCR places on an accurate risk analysis that identifies all places within a system that ePHI resides," Hodge stated. "To avoid shared settlement payments, covered entities that permit shared access to ePHI should closely read the NYP and Columbia resolution agreements and implement the described action items."

Lesson #2: Whatever You Do, Don't Skip the Risk Analysis

According to associate attorney **Jefferson Lin** in a May 13 blog posting for the Seattle-based law firm **Ogden Murphy Wallace Attorneys**, the CAP for each provider requires both entities to:

- Conduct a comprehensive and thorough risk analysis;
- Develop and implement a risk management plan;
- Review and revise policies and procedures on information-access management, as well as device and media controls;
- Develop an enhanced privacy and security awareness training program;
- Provide progress reports; and

CPT® 2023 American Medical Association. All rights reserved.

Develop a process to evaluate any environmental or operational changes that impact the security of ePHI (CU only)

"This settlement again highlights the necessity for healthcare organizations and business associates to create and implement security policies and procedures, and to engage in a security management process that ensures the security of patient data," Lin wrote.

Lesson learned: "The message here is to be sure you use good, professional practices in the development and implementation of all systems handling PHI," stresses **Jim Sheldon-Dean**, founder and director of compliance services at **Lewis Creek Systems, LLC** in Charlotte, VT.

Links: To read the NYP's Resolution Agreement, go to www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/ny-and-presbyterian-hospital-settlement-agreement.pdf. CU's Resolution Agreement is at www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/columbia-university-resolution-agreement.pdf.

CPT® 2023 American Medical Association. All rights reserved.