Health Information Compliance Alert

Case Study: How Much Could You Pay For Your BA's Mistakes?

Why you're increasingly at risk for breach-related private lawsuits.

Finger-pointing will get you nowhere when you have a HIPAA breach. And one recent case demonstrates how you could end up paying through the nose for your business associate's (BA's) HIPAA violation.

Background: Led by former patient **Shana Springer, Stanford Hospital & Clinics** and two of its vendors faced a class action lawsuit for alleged privacy breaches of patients' protected health information (PHI), violating California's state privacy laws. The plaintiffs sought $20 million in damages, but the defendants recently settled the case for $4.1 million.

Multi-Specialty Collection Services LLC (MSCS) was Stanford's BA and was named in the lawsuit, and then another BA contracting with MSCS, **Corcino & Associates LLC**, was added to the complaint. The lawsuit alleged that Stanford and its BAs were responsible for disclosing the PHI of 20,000 emergency room patients. The BA actually posted an Excel file online containing the PHI.

Because the BAs were at fault for the unpermitted disclosure, they will pay the majority of the settlement about $3.3 million, reported attorney **Elana Zana** in a March 27 blog posting for the Seattle-based law firm **Ogden Murphy Wallace**. But Stanford is still stuck paying out a whopping $500,000 toward a "vendor education fund" under the settlement agreement, as well as $250,000 in settlement administrative costs.

Why 'No Fault' Doesn't Protect Your from Lawsuits

And keep in mind that this settlement arose strictly from violations of state privacy laws. The state and federal government investigated the incident and determined that Stanford was not at fault for the disclosure, stated **Martie Ross**, attorney and principal for Pershing Yoakley & Associates (PYA), in an April 4 PYA Healthcare Blog posting. Stanford received no penalties or fines.

Beware: "The risks of private lawsuits are real," Ross warned. Just because HIPAA does not include a private cause of action doesn't mean that patients cannot sue you under state law.

"Many states, like California, have privacy laws that allow a private individual to sue a party that violates that law," Ross noted. "Additionally, an individual can bring a common law claim for negligence, alleging a HIPAA breach violates the standard of care.

Hidden trap: And now that HIPAA requires you to notify patients of breaches, there are more opportunities for affected patients to pursue private claims, Ross said. Attorneys may not care much about a single patient's complaint, but breaches usually involve a larger number of patients. And this can lead to a class action lawsuit with a potentially large payout, which is enticing to plaintiffs' attorneys.

Crack Down on Your BA's Actions

"Looking at the facts as reported, it is hard to find anything Stanford did wrong," Ross lamented. Stanford had an appropriate BA agreement (BAA) in place, "it had no notice of any prior wrongdoing by MSCS, it encrypted the data sent to MSCS, and it met its obligations with respect to mitigation and breach notification once the posting was discovered."

Stanford was even unaware of Corcino, which contracted with MSCS, and ultimately was directly responsible for the breach, Ross noted. "So why is Stanford paying out $750,000?"

CPT® 2023 American Medical Association. All rights reserved.

"Not only is Stanford its brother's keeper, it is also its brother's brother's keeper," Ross said. Thanks to the HIPAA Omnibus Final Rule, there is now a greater emphasis on BAs' and subcontractors' responsibility to protect patient privacy.

Bottom line: "The major lesson to glean from this case is that covered entities should better investigate their vendors before transmitting PHI," Zana stressed. "Meaning not just simply executing a Business Associate Agreement with an indemnification and insurance provision (though advisable), but also reviewing/evaluating their current security policies, staff training, use of subcontractors, and encryption standards."

CPT® 2023 American Medical Association. All rights reserved.