HIPAA Regulatory Alert
Cutting-edge information on privacy regulations

Physician's tinkering causes data breach, record $4.8 million in HIPAA settlements

Two prominent New York organizations have agreed to pay $4.8 million to settle charges stemming from a data breach, and they take the dubious honor of the largest settlement ever for violating the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. The breach has been traced to the actions of a single physician who had access to a computer server.

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) says the providers failed to secure thousands of patients' electronic protected health information (PHI) held on their network. A major lesson from the breach is that partnering with another provider brings substantial risk if you do not thoroughly assess how data will be shared and protected.

OCR initiated its investigation of New York — Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated Sept. 27, 2010, regarding the disclosure of the PHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results. NYP and CU are separate covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP. The entities generally refer to their affiliation as "New York Presbyterian Hospital/Columbia University Medical Center."

NYP and CU operate a shared data network and a shared network firewall that is administered by employees of both entities. The shared network links to NYP patient information systems containing PHI. The breach did not happen in any of the most typical ways, such as a laptop being lost or stolen. Instead, a single physician mistakenly thwarted NYP and CU's security systems.

The OCR investigation revealed that the breach was caused when a physician employed by CU, who developed applications for NYP and CU, attempted to deactivate a personally owned computer server on the network containing NYP patient PHI. Because of a lack of technical safeguards, deactivation of the server resulted in PHI being accessible on internet search engines, the OCR reports. The entities learned of the breach after receiving a complaint by an individual who found the PHI of the individual's deceased partner, a former patient of NYP, on the internet.

In addition to the impermissible disclosure of PHI on the internet, OCR's investigation found that neither NYP nor CU made efforts prior to the breach to ensure that the server was secure and that it contained appropriate software protections.

"Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP PHI," OCR stated in announcing the settlement. "As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of PHI. Lastly, NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management."

Must assess risk of working with partner

NYP has paid OCR a monetary settlement of $3.3 million, and CU has paid $1.5 million. Both entities agreed to a substantive corrective action plan, which includes undertaking a risk analysis, developing a risk management plan, revising policies and procedures, training staff, and providing

EXECUTIVE SUMMARY

Two organizations will pay a combined $4.8 million to settle a case sparked by a breach of protected health information (PHI). The settlement is the largest ever for a violation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- The breach involved the PHI of 6,800 people.
- A physician caused the breach by accessing a server.
- Partnering with another provider brings substantial risk if you do not thoroughly assess how data will be shared.

progress reports. (The New York — Presbyterian Hospital Resolution Agreement may be found at http://tinyurl.com/lakqm96. The Columbia University Resolution Agreement may be found at http://tinyurl.com/ofyargl.)

The incident and the large settlement figure illustrate the risk that healthcare providers take on when working on such a data-driven project with another provider, says **Alisa L. Chestler**, JD, shareholder with the law firm of Baker Donelson in Washington, DC. "You have two entities here that were collaborating to do really good work, but even the most minute details of how you create, receive, transmit, or maintain information needs to be understood," Chestler says. "This employee of one essentially compromised them both by trying to terminate access in a way that obviously didn't work. This shows that you have to ask what you know about what your partner is doing and how they're doing it."

A thorough risk analysis is necessary for any partnership involving data sharing, Chestler says. Both of the corrective action agreements in this case call for a risk analysis.

Risk analysis failure can be your downfall

The risk analysis failure turned out to be as important to this case as the breach itself, which did not involve as many patients as some previous breaches, says **Brad Rostolsky**, JD, an associate with the law firm of Reed Smith in Philadelphia. One sure lesson from the New York case is that you want to stay out of the government's way as much as possible, he says. Once OCR investigated the breach, it found overall deficiencies in HIPAA compliance.

"If they look at you for HIPAA compliance purposes and determine that you have not conducted an appropriate risk assessment under the security problem, there's going to be a problem," Rostolsky says. "Notwithstanding everything you may be doing with HIPAA compliance, if you have not conducted an appropriate risk assessment, you are going to be in trouble if the government finds out."

A key term there is "appropriate." OCR investigators will not look kindly on a risk analysis that seems perfunctory or trying to meet minimum expectations, Chestler says.

"Your risk analysis cannot be a 'check-the-box-and-move-on' exercise," she says. "You may be working with a partner that has a stellar reputation and you have every reason to think their data security plan is top notch, but you still have to go through the due diligence of looking at how data is handled. I'm sure in this case both parties thought they had adequate controls, but there was a fault in the system."

Chestler sees still another message in the New York settlement. OCR is pursuing HIPAA violations with vigor in a wide range of healthcare settings, from small government entities to huge private sector companies such as Wellpoint and these New York entities, she notes. "They are clearly trying to send a message that they are taking a broad approach to enforcement so that no one, large or small, starts to feel that they are under the radar," Chestler says. "There are going to be a lot more settlements like this one. Whether you're a big system or a small provider, nobody is immune."

OCR is becoming more aggressive in enforcing HIPAA and the hopscotching from private to government entities, big to small, is making their actions hard to predict.

Interestingly, the resolution agreements call for more specific training of employees and physicians, Chestler says. She sees that as a warning that OCR is expecting more detailed training tailored to your own organization rather than generic HIPAA education. "I don't think those off-the-shelf HIPAA education programs are going to work anymore," she says.

SOURCES

• **Alisa L. Chestler**, JD, Shareholder, Baker Donelson, Washington, DC. Telephone: (202) 508-3475. Email: achestler@bakerdonelson.com.
• **Brad Rostolsky**, JD, Associate, Reed Smith, Philadelphia. Telephone: (215) 851-8195. Email: brostolsky@reedsmith.com. ■

Desk audits are coming, but what are they like?

The Department of Health and Human Services (HHS) Office of Civil Rights (OCR) will begin conducting desk audits for Health Insurance Portability and Accountability Act (HIPAA) compliance this fall, which has many providers wondering just what they will be like. Most HIPAA experts expect the desk audits to be relatively pain-free, but until someone goes under the microscope, no one can be sure.

OCR is selecting a sample of covered entities, which includes hospitals and other medical service providers, to perform desk audits. OCR has started contacting 500-800 covered entities in preparation to survey these entities this summer. From that 500-800 entity survey group, OCR is going to select 350 covered entities on which to perform desk audits. Some hospitals will be