Report on
Patient Privacy

Volume 14, Number 2 • February 2014

Practical News and Strategies for Complying With HIPAA

Strategies to Thwart Human Error Help Ensure HIPAA Compliance, Limit Breaches

In 2012, hackers downloaded files with protected health information (PHI) for nearly 800,000 Utah residents after a contractor forgot to reactivate a firewall *(RPP 6/12, p. 3)*. A similar deed two years earlier, also involving a non-working firewall, mistakenly exposed the PHI of 17,000 patients treated by Idaho State University to potential misuse, a situation that ultimately cost ISU a $400,000 settlement with the HHS Office for Civil Rights (OCR) *(RPP 6/13, p. 1)*.

Also in 2010, a neurologist and researcher visiting South Korea to deliver a lecture perhaps absentmindedly put his backpack down in a public place. When he went back to look for it, the backpack, and the unencrypted laptop inside containing PHI for some 3,500 patients and research subjects, were gone. The OCR investigation triggered by the theft resulted in a $1.5 million settlement *(RPP 10/12, p. 1)*.

It's a truism that technology is a powerful tool that HIPAA covered entities (CEs) and business associates (BAs) can, and often should, deploy, as part of a compliance program backed by policies and procedures. But as these three incidents show, sometimes forgetful, distracted and untrained human beings continue to make "errors" that may lead to governmental wrath, and sometimes financial penalties, not to mention bad public relations.

"Human error increases risk when there are already vulnerabilities in place," OCR spokeswoman Rachel Seeger tells *RPP*.

Rebecca Fayed, associate general counsel and privacy officer for The Advisory Board Company, which is business associate to hospitals and health systems, said the threat of misdeeds by hackers and other outsiders can be overstated. "My opinion is those threats are far less common across the industry than the simple mistakes people make trying to do their jobs, when they do not know what is required, or can't remember what is expected," Fayed told *RPP*.

For example, the two incidents that resulted when firewalls were not reactivated could have been prevented had employees been following a "checklist" for the upgrades or repairs they were making. The second to the last item on the checklist might have been "reactivate firewall," while the last item should have been "run a test," according to Mac McMillan, co-founder and CEO of CynergisTek, Inc. and chair of the HIMSS Privacy & Security Policy Task Force.

The use of simple checklists are among the combination of strategies that can reduce "vulnerabilities" to tamp down on human error. Others, according to McMillan, include: privacy, security and breach policies that will really work when put into practice and are reviewed to make sure are functioning properly; an environment that encourages employees to ask questions before they make a mistake and to share slip-ups with compliance officers when they do; and the careful deployment of technology that employees aren't able to circumvent.

Since the privacy rule went into effect in 2003, impermissible uses and disclosures of PHI are the top HIPAA compliance issue that OCR has investigated, according to Seeger. So it's easy to see how often the human element comes into play.

The role employees have in compliance demands a real focus, Fayed said. "We place a great deal of effort on understanding that your employees are your greatest asset, but they can impose significant liability if they don't know what is expected of them," she said. "We always say we are only as strong as our employees — including the ones we just hired yesterday."

She believes compliance programs have the best chance of succeeding if they don't put unnecessary, or unintentional, roadblocks in the path of employees. "Make it easy to comply," Fayed said. This begins with marrying necessary safeguards and practices to the activities that employees engage in on a daily basis. Fayed, an attorney who was in private practice for 10 years prior to joining The Advisory Board in 2011, said she makes it her business to attend different "team meetings" within the company so that she understands all the firm's functions.

"You want to know the people who have their ears to the ground," she said. "You will learn from them." When the time comes to develop a new policy or procedure, those individuals serve as a necessary sounding board.

A compliance officer needs to know that "what you are setting out in the form of a policy actually works on the business side," she said. Fayed will explain to staff: "'This is what the law says. This is what I am thinking. Does this actually make sense?' Take their comments into account so you are not hit with resistance" once a policy is in place, she recommended.

"From a practical standpoint…the business and compliance teams have to work together. Otherwise, [employees] are just going to work around" whatever the policy says, and that's when violations can occur, Fayed pointed out. For example, many CEs and BAs, including The Advisory Board, now have blanket policies that require encryption of laptops, which Fayed called "hard to argue with." But The Advisory Board also prohibits PHI from being stored on even encrypted laptops, except temporarily under special and limited circumstances.

Employees can be granted a "security exception" that takes into account the "risk and the need" for short-term storage of the PHI, she said. For example, an employee may need to bring data to a meeting. These exceptions may be granted by the Advisory Board's Information Security Group, provided certain conditions are met, including ensuring that appropriate safeguards are in place and there is a legitimate business need that cannot otherwise be met, Fayed said.

Frank Ruelas, a long-time HIPAA compliance officer currently at Gila River Healthcare in Arizona, and principal of HIPAA College, also shared with *RPP* his experiences in addressing the issue of human error. He and Fayed offered the following recommendations:

◆ ***Keep an "open door" and encourage "self-reports."*** According to Fayed: "I have had people self-report mistakes. For example, an employee might email PHI, which is a violation of the Advisory Board's policies but not HIPAA. I tell them 'It's a much better situation if you come forward yourself, quickly. Call me, alert me, the minute it happens,'" so the firm can take action to mitigate any potential effects of whatever went wrong. Generally speaking, time is often of the essence when a serious incident may have occurred, she warned.

◆ ***Encourage reporting by other employees.*** It is important that CEs and BAs ensure they have "zero tolerance" for any supervisor or coworker retaliating against a workforce member who brings a HIPAA issue to officials' attention. There can be no repercussions for a "good-faith report" being filed, Ruelas says. For workers to get this message, "it took the termination of several people who tested the system" by retaliating, he said.

◆ ***Keep digging.*** When investigating a possible HIPAA violation, Ruelas tells the worker, "I need to understand what you were thinking." The statement, "I made a mistake" isn't an explanation. Asking "Were you working too quickly? Were you distracted?" may help elicit the real reason something went wrong, Ruelas said. Asking "why" each time the worker gives an answer is a useful strategy he frequently employs to draw out more information *(RPP 6/10, p. 1)*.

◆ ***Address common reasons for the missteps.*** Like Fayed, Ruelas said the explanations he often hears are that employees "didn't know the process, they didn't get training and they didn't have people to help them." Once known, strategies should be developed to address these issues. Fayed recommended working directly with the employee in a "team approach" to mitigate a problem when possible.

◆ ***Find and fix "pockets of wrongness."*** Among organizations, particularly those with many long-timers, bad habits, sloppiness and outright HIPAA violations might have become the norm. When investigating an incident or complaint, ask the question: "Is there a pocket of wrongness in this department?" Ruelas suggested. Then take appropriate actions, which might include selective retraining.

◆ ***Audit compliance.*** Despite all the homework that is done before they are implemented, some policies and procedures are still going to fail in real life. So constantly monitor compliance, be open to changes and make revisions when necessary, Fayed said. Policy development "is a continuous process," she added. Gila River decided two years ago that every policy will have "some type of auditing and monitoring associated with it," according to Ruelas.

◆ ***Deploy technology that automates compliance.*** "If there is a human element" involved in the compliance activity, there is a "residual risk" that threatens successful completion, Ruelas said. When possible, technical solutions that cannot be overridden should be implemented. For example, Gila River prohibits downloading of PHI onto unencrypted USB drives, and now makes available for use only drives that self-encrypt.

◆ ***Implement administrative fail-safes.*** "We have caught people on the floor without training," Ruelas said. To address a lack of training among new workers, for example, institute an automated step in payroll procedures that prevents payment from being issued until there's a certification that training has been completed, he suggested.

◆ ***Counsel caution.*** Ruelas likes to remind employees that they don't have to respond to a request for PHI they're not sure about, or take some action they're not certain is allowed by HIPAA. "There is nothing that has to happen immediately," he said. Advising workers that it is OK to slow down, ask a question and get an answer before acting can be "a huge relief" to an employee who feels under pressure, Ruelas said.

Contact Fayed at FayedR@advisory.com and Ruelas at frank@hipaacollege.com. ✧