NETWORKWORLD

Warning: HIPAA has teeth and will bite over healthcare privacy blunders

New government fine structure plus random auditing make healthcare privacy lapses even less acceptable

By Tim Greene and Ellen Messmer, Network World
September 09, 2011 09:13 AM ET

Healthcare organizations that are performing risk assessments as a way to craft patient-privacy policies might want to consider a new potential attack vector: federal regulators.

Later this year, the Department of Health and Human Services is expected to start auditing up to 150 health providers at random through December 2012 in an effort to find medical entities that fail to comply with HIPAA and HITECH regulations about how personal data must be handled securely.

IN THE NEWS: Stanford Hospital investigating patient data leak

While the audits don't represent attacks on the personally identifiable information (PII) the regulations are supposed to protect, they do expose non-compliant providers to the potential for heavy fines and reputation-damaging publicity.

For instance, earlier this year Massachusetts General Hospital paid $1 million to settle a patient-privacy complaint with HHS due an employee leaving patient records in a subway car.

That's a big switch from the way healthcare privacy regulations have been handled since 2003, says Abner Weintraub, president of HIPAA Group, a compliance consultancy to healthcare organizations. Until this year, HHS had received about 50,000 complaints but levied no fines, preferring to take remedial actions instead, he says.

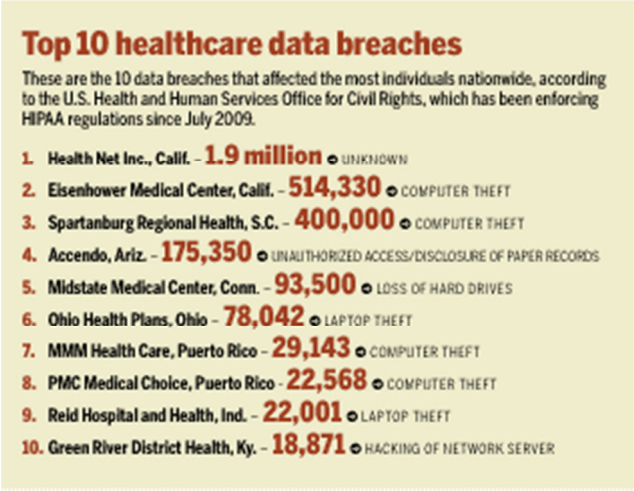
Levying fines now has an upside for HHS, says Kelly Hagan, a healthcare attorney with law firm Schwabe, Williamson & Wyatt in Portland, Ore. - the agency gets a cut of whatever fines are levied. That, combined with the pro-active auditing, marks a sea change for what healthcare CIOs and CISOs face when dealing with HIPAA. "Suddenly HIPAA has teeth and is willing to bite," Hagan says.

Despite this, instances of healthcare data breaches continue to flourish. Just this week, it was revealed that emergency room records from Stanford Hospital in Palo Alto, Calif., were posted for most of a year on a Web site where students can hire help to do schoolwork.

MORE ON HEALTHCARE TECHNOLOGY:

Last year, HHS received 207 reports of breaches involving more than 500 individuals, according to areport to Congress last week. And there are growing incentives for criminals to focus on health record theft, Weintraub says. Patient data can be sold to criminals interested in perpetrating identity theft, he says, but more lucrative are schemes to commit medical identity theft.

That's when stolen patient data is used to obtain medical care for someone else, which not only bilks insurers but also taints the medical record of the individual whose identity is stolen by inserting records of treatments and tests the victim never received.



Medical organizations need to think of themselves not as repositories of neutral data but as protectors of valuable assets, he says. "Rather than a library, they have to think of themselves as running a bank," he says, and that may include using security cameras and guards to defend certain medical records.

While some of the challenges healthcare IT executives face are technical. Many medical applications, by nature, require low latency and sharing of PII. So the network environment makes it somewhat hard to apply security controls, such as firewalls, which can slow things down and create performance issues for imaging applications, says Jeff Bills, vice president of IT at Solutions Healthcare Management, a consultancy and technology provider headquartered in Indianapolis.

But many of the security issues have to do with people. Data breaches may be the fault of staff or of business associates working on behalf of a healthcare provider, says Amit Trivedi, healthcare program manager at ICSA Labs. "Data breaches are often a result of breakdown of processes and controls, or lack of them altogether," he says.

In talking to his clients, Bills warns about employees as a risk. "What we try to drill into them is that you can put up all the firewalls, anti-malware and intrusion prevention you want for the outside of your network, but you are your own enemy on the inside of your network," he says.

While it falls outside the traditional purview of IT executives, training of staff and creating an atmosphere of privacy must be addressed to meet HIPAA regulations. Policies and procedures for dealing with PII are essential, Weintraub says.

That requires the help of healthcare executives and human resources departments, says Susan Patton, a healthcare attorney with Butzel Long in Detroit. "There's a limit to what IT can do when the problems are really caused by human mistake," she says. "It's hard to fix human nature with IT."

She advocates creation of a culture of confidentiality. "Privacy must be seared into that part of the brain used for dealing with the patient," she says.

Which is pretty much what HIPAA calls for, Weintraub says. The policies and procedures that the law requires healthcare organizations to write must also be taught to employees in a way they can understand and put in practice, he says.

Meanwhile, the IT staff should focus on general security best practices that are applied in all industries rather than trying to craft practices to satisfy HIPAA, because the two overlap greatly he says. "If you've done everything you should be doing anyway to protect your network and data, you're going to be largely compliant with HIPAA from the get-go," he says. "The challenges are still the same old set of vulnerabilities and ignorance."