September 15, 2008

A HIPAA Crackdown?

By Selena Chavis
For The Record
Vol. 20 No. 19 P. 24

As consumers become more aware of privacy issues, some experts are warning covered entities to expect greater scrutiny, while others suggest that new efforts still don't address the bigger picture.

This July marked a milestone in the HIPAA saga. For the first time since the privacy and security rules were enacted, a covered entity was required to pay a fine.

Seattle-based Providence Health & Services agreed to pay $100,000 as part of a settlement with the Office for Civil Rights (OCR) and the Centers for Medicare & Medicaid Services (CMS) that resulted from a joint investigation following the receipt of 31 complaints.

Add to that what appears to be an escalation in the criminal prosecution of HIPAA-related cases by the Department of Justice (DOJ), and many experts are left wondering if these recent events mark a turning point in HIPAA enforcement—an effort that has been primarily characterized by voluntary compliance efforts through the issuance of corrective action plans to covered entities.

"There is definitely an uptick in HIPAA enforcement," says Mark Rogers, a Boston-based healthcare attorney. "They [Health and Human Services (HHS)] are a lot tougher now when they come in to do their investigations. It was the number of instances and the amount of information that made Providence the poster child."

The Providence example is certainly unique, but a spokesperson with the OCR is quick to point out that the outcome is not a civil monetary penalty but a formal resolution agreement accompanied by a more stringent corrective action plan that has typically been issued in the past. Under the plan, the healthcare system is required to revise policies and procedures, improve the management of off-site transport and storage of electronic media, train staff regarding the new safeguards, and submit compliance reports to HHS for three years. The organization will also be subject to audits and site visits.

The action represents a notable step for many critics of the privacy and security rules who suggest that the enforcement has not been steep enough to truly get the attention of the healthcare community. Others suggest that corrective action plans have been appropriate due to the fact that the majority of the complaints requiring action are basically for "sloppy security" practices.

"People want to see OCR take a more aggressive stand. ... But are you going to slap a criminal penalty on a healthcare organization for a minor infraction they are willing to fix?" questions Dennis Melamed, president of Melamedia, publisher of Health Information Privacy/Security Alert, an industry trade newsletter.

As of June 30, the OCR had received more than 37,200 complaints, 80% of which had been resolved. Of those, 6,648 cases were deemed appropriate for investigation and resolved through corrective action plans. The others were either considered out of the HIPAA scope of jurisdiction, unfounded, or referred to other departments.

Is the Honeymoon Over?

The OCR says that more activity such as the resolution agreement at Providence is likely to happen.

"It's fair to say that in the first year or so, we were using education and technical assistance with covered entities to get them into compliance, but it's also true that covered entities should be taking responsibility for compliance now," says Susan D. McAndrew, JD, deputy director of health information policy for the OCR. "Enough time has passed for entities to know what their obligations are, and we have a variety of compliance tools that we are willing to use."

HIPAA's scope allows for civil monetary penalties of up to $100 per violation and up to $25,000 per year for each requirement or prohibition violated. Criminal penalties apply for certain actions, such as knowingly obtaining protected health information in violation of the law, and are referred to the DOJ.

Criminal penalties can reach up to $50,000 and one year in prison for certain offenses, up to $100,000 and up to five years in prison if the offenses are committed under "false pretenses," and up to $250,000 and 10 years in prison if the offenses are committed with the intent to sell, transfer, or use protected health information for commercial advantage, personal gain, or malicious harm.

As of June 30, 436 cases had been referred to the DOJ, but only a handful of cases had actually involved prosecutions. Recent DOJ cases such as the one involving Andrea Smith, a licensed practical nurse in Arkansas who pled guilty to wrongfully disclosing patient information for personal gain, suggests to some experts that the tides may be changing.

Rogers suggests that the electronic health record (EHR) movement will further intensify efforts for more stringent HIPAA enforcement as the general public demands more protection. "I tell my clients that the honeymoon is over. OCR gave an appropriate period of time where everyone started to adjust to the rules," he says. "It's the adoption of the EHRs. You put all the pieces of that together, and the government is saying we have to protect the consumer."

However, according to Melamed, the reality of the minute number of HIPAA prosecutions suggests a deeper issue in that the HIPAA complaint system has played little or no role in uncovering criminal conduct. "I have yet to see a case where a complaint from OCR led to a criminal indictment by DOJ," he notes.

Melamed further suggests that, moving forward, the bulk of criminal enforcement activity will occur on the state level.

"Now we're in a situation where the states are filling the void," Melamed says, pointing to the frustrations of those with complaints who cite their inability to sue under HIPAA. "There have been a host of state laws enacted in recent years, and the states discovered they had many laws already on the books. People are going to the state courts."

Inconsistent privacy and security laws on the state level are creating problems of their own, however, since it becomes difficult to exchange patient information across state lines. Melamed suggests that this will further complicate the electronic movement in healthcare.

Rory Jaffe, co-chair of the California Privacy and Security Advisory Board, agrees, noting that he sees privacy issues impacting and deterring the larger health information exchange effort rather than the EHR movement.

"It's getting difficult to track where the information is and whether you can trust your partners," he says. "We're in a fairly unstable part of this whole thing. … It will certainly all shake out."

What Did You Expect?

That's the question Melamed raises when critics point fingers at HIPAA, questioning why the rules have not produced more notable civil and criminal results.

"What do you expect from OCR?" he says. "They weren't set up to be the criminal enforcement guys. Their focus is on policy and procedure."

HHS believes that part of the misunderstanding surrounding HIPAA enforcement rests with the fact that there are big misconceptions about the rule's jurisdiction and scope.

Enacted to regulate the use and disclosure of individually identifiable health information, HIPAA privacy and security rules, on the surface, provide the first and only national standards for protecting the privacy of health information. Among other provisions, it gives patients more control over their health information, sets boundaries on the use and release of health records, and establishes appropriate safeguards that the majority of healthcare providers must achieve.

But the scope of the OCR and the CMS is limited, and statistics reveal that the vast majority of complaints received by these departments either do not warrant severe action, are unfounded, or do not even fall under HIPAA jurisdiction, says Jaffe.

"I don't think criminal enforcement for the majority of issues [related to complaints filed with HIPAA] would beef things up much," he says. "Certainly there should be a lot more sanctions for people doing this for financial benefit or to cause harm … but that's the minority of [cases] we are seeing."

It's the high-profile breaches that make the evening news and draw focused attention to the need for greater patient privacy safeguards, Melamed says. But the OCR is quick to point out that much of the malicious activity that makes headlines is outside HIPAA's

scope.

"If there were systems or practices by covered entities that made them vulnerable to a breach, that would fall under HIPAA," says McAndrew, adding that for a complaint to be filed, the general public would have to be aware that such a vulnerability existed. "To the extent that a covered entity is not appropriately and effectively protecting patient privacy, that would fall under HIPAA," she says.

That's where HIPAA has a huge blind spot, according to Jaffe, because "HIPAA only covers three types of entities—providers, clearinghouses, and health insurers." Melamed adds that since those three entities must use electronic transactions, the rule is even more limited.

Reaching a Moving Target

Greater visibility of breaches and malicious efforts to steal patient information, such as the incident in which 26 million records were stolen at the Department of Veterans Affairs, will continue to raise public concern, says Melamed.

"We are starting to see a slight uptick generally in the number of cases filed with OCR," he says. "It's a general concern over the nature of the breaches being reported."

He further suggests that focusing on the OCR and the CMS alone will not provide a complete picture of what is really happening because other federal agencies have some health data privacy enforcement responsibilities that go beyond HIPAA's limited world.

A spokesperson at the OCR points out that an analysis of statistical data since HIPAA was enacted may support the need to expand the statute's scope or develop some other strategy for ensuring proper consumer protection as it becomes more and more apparent that many areas of the healthcare system are not covered by HIPAA.

Consider the definition of a covered entity, Melamed says. Because HIPAA covers only providers, health insurers and plans, and healthcare clearinghouses, others such as Google or Microsoft are not governed by HIPAA. There are also the pharmaceutical companies to consider, and the list goes on and on.

"The focus of HIPAA is shortsighted and myopic. The way we regulate healthcare data is above and beyond HIPAA," Melamed says, suggesting that what is missing is comprehensive privacy legislation. "It's an incomplete set of instructions that might not have been aimed at the right people."

Melamed says the controversies surrounding HIPAA's effectiveness bring up a number of questions and considerations that apply to the greater scheme of privacy protection.

First, he points out that healthcare makes up a huge portion of the U.S. economy and is much broader than just hospitals and doctors. He questions whether the privacy rule is truly aimed at all the right entities, adding that the lack of enforcement—or the lack of complaints warranting the need for civil monetary penalties—may point to an inherent culture within healthcare that is focused on privacy.

"Was healthcare the hotbed of abuse that we all assumed it was?" he asks. "It's too narrow a segment."

On the other side of the picture, he says the complaint system is passive—it's government bodies waiting for consumers to lodge concerns when they may not have the awareness or knowledge to know what constitutes a poor security practice.

"You can file with OCR, but there's really nothing in it for you," he adds, pointing to the fact that people can't sue under HIPAA. "Don't expect gratification."

Jaffe says regardless of whether HIPAA has addressed the criminal side of privacy breaches effectively, there is still a range of activity where criminal enforcement has a place. "Given the spectrum of reasons for why people access health records, there is definitely a role for law enforcement," he says. "It's fighting a different battle that we've had with other policies and procedures. The typical institution is nowhere near perfect in protecting a patient's information."

As the electronic movement continues to gain momentum, Melamed believes the big question moving forward will become, "Who is going to have stewardship for protecting people's privacy?"

An OCR spokesperson points out that even with its limited scope, HIPAA was an important step to lay the groundwork for privacy regulations, adding that privacy and security standards will continue to improve harmful practices, especially as EHR concerns heighten awareness.

— Selena Chavis is a Florida-based freelance journalist whose writing appears regularly in various trade and consumer publications covering everything from corporate and managerial topics to healthcare and travel.