



BUSINESS

Practices must have plans for handling health data breaches

Time is running out for physicians to comply with notification requirements that go into effect Sept. 23.

By PAMELA LEWIS DOLAN, AMNews staff. Posted Sept. 14, 2009.

PRINT | E-MAIL | RESPOND | REPRINTS | SHARE



Follow Whether you are a solo physician

in a small rural setting or an employed physician in a large urban hospital, starting Sept. 23, if patients' personal data are leaked, you have to let them know.

This could mean sending a letter to the patient or patients affected or taking out a quarter-page ad in the local newspaper, depending on the type of breach. Additionally, even if a breach never occurs, the new rules require practices to have a plan in place -- just in case.

- [AMA guidelines on breaches](#)
- See [related content](#)

The new breach notification rules, sanctioned by the American Recovery and Reinvestment Act, were issued by the U.S. Dept. of Health and Human Services in August.

"I think what the rules are saying is, you are not really going to be able to stick your head in the sand and say, 'OK, I am not dealing with this.' You're going to have to roll up your sleeves and deal with it in a very proactive way," said attorney Andrew Blustein, co-chair of the HIPAA-compliance group at the law firm Garfunkel, Wild & Travis, which has offices in Connecticut, New Jersey and New York.

Although some states have notification laws, many physicians are facing this requirement for the first time.

Privacy breaches involving more than 500 patients must be immediately reported to HHS and the media.

Attorney Steven Eisenberg, partner with national law firm Baker Hostetler, said a practice's first course of action should be to re-examine its privacy and security policies to ensure they reflect current law. With fines that could reach up to \$1.5 million for a breach, and the potential for criminal and civil action against individuals, now is a good opportunity for practices to retrain staff members to ensure that they know

what's allowed and what could get them into trouble.

Eric Nelson, a consultant with Newport Beach, Calif.-based Lyndon Group, said that under the law, each practice must have a documented risk assessment on file that details what information might be vulnerable and what the practice is doing to mitigate that risk. Nelson said HHS has the authority to audit practices to ensure this assessment has been conducted.

Practices also must develop a breach response plan. Because different types of breaches require different actions, the plan should detail the responsibility of key players for every potential type of breach.

Attorney Janice Anderson, partner in the health care practice at Polsinelli Shughart in Chicago, advises practices also to re-evaluate contracts with business associates when developing a response plan so it's clear who will assume what responsibilities in the event of a reportable breach.

The type of notification, and even if notification will be required, will depend largely on how many people were affected and what safeguards were in place. Not every breach falls under the notification requirements.

In the final rules, a breach is defined as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information."

But "even though it may seem like a breach off the cuff, the breach actually has to relate to

some level of harm," Day said. If stolen data were unreadable or inaccessible either because they were destroyed or rendered useless, there is no harm under the law. Therefore, if a laptop with encrypted data were stolen, for example, "there would be no further duty," he said.

The rules also define what to do in case employees see information they are not supposed to view. Depending on the circumstances, a breach might not have to be reported.

For instance, if an office employee sends an e-mail with personal health information to the wrong recipient inside the practice, and that recipient does not access the file, or if a nurse opens the wrong patient file inadvertently, realizes the mistake and closes it immediately, then it is likely the practice would not have to inform patients. But if there is an HHS audit, the burden is on the practice to prove there was no harm, Blustein said.

It is a reportable offense if an employee intentionally gains access to files they are not authorized to look at.

Unlike former HIPAA rules that did not specify a time frame for action to be taken post-breach, the new rules give very specific deadlines. The law says the practice should take action immediately, no later than within 60 days.

Breaches involving more than 500 people require immediate notification of HHS and the media. In cases involving fewer than 500 patients, each breach must be recorded in a breach log that is sent to HHS annually.

The law also is very specific in terms of how patients are to be notified. If a third-party business associate is responsible for the breach, that party's only must report it to the practice. The practice then must assume responsibility for alerting patients.

Notification letters have to include information on exactly what happened, what the practice is doing to protect the victims, what actions victims can take to further protect themselves, and a number to call for more information.

Other specific requirements apply to cases in which letters are returned for the wrong address, or the patient is deceased.

The policies go into effect Sept. 23, so experts advise immediate action. "The government has not given us a lot of time," Blustein said.

This content was published online only.

[BACK TO TOP](#)

ADDITIONAL INFORMATION:

AMA guidelines on breaches

At its Annual Meeting in June, the American Medical Association House of Delegates approved guidelines on patient data breaches, before the HHS rules were announced. The AMA guidelines say that in case of a breach, physicians should:

- Ensure patients are properly informed.
- Follow ethically appropriate procedures for disclosure.
- Support responses that place the interests of patients above those of the physician, medical practice or institution.
- To the extent possible, provide information to patients to enable them to diminish potential adverse consequences of the breach.

[BACK TO TOP](#)

Copyright 2009 American Medical Association. All rights reserved.

RELATED CONTENT

- » [Doctors prepare for ID theft rules](#) May 18
- » [Stimulus package alters HIPAA rules for business associates](#) Column May 4
- » [Laws bolster penalties for privacy breaches in California](#) Dec. 1, 2008