JOURNAL OF AHIMA

FEBRUARY 2010

Breach Notification Scenarios

In September 2009 the Department of Health and Human Services released an interim final rule describing a covered entity's responsibilities to notify victims of a breach to their personal health information. The new rule was the result of provisions in the American Recovery and Reinvestment Act. Penalties for noncompliance take effect February 22, 2010.

How well do you know the ins and outs of the rule? It's complicated, and there are many moving parts. Test your knowledge on the four following breach scenarios. Select the one best answer for each scenario. Each correct answer is based directly on a given section of the rule.

Scenario 1

Inadvertent disclosure of deceased patient information

General Hospital recently provided Mr. J. Smith with a copy of his complete medical record from his last visit. Accidently contained within the copies was the history and physical report of Robert Lewis. Mr. Smith, who is dissatisfied with General Hospital, called the HIM department to report the misdirected history and physical, complaining that the mistake was just another example of the substandard practices at General Hospital.

Mr. Smith refused to return the history and physical. He insisted he would call Mr. Lewis personally to inform him of the hospital's incompetence. Further investigation revealed that Mr. Lewis is deceased. The hospital's records do indicate the name and address of Mr. Lewis's next of kin. In response to this breach the hospital should:

a. Do nothing, because Mr. Lewis is deceased.
b. Notify the hospital attorney. Secure a court order and seize the records from Mr. Smith.
c. Notify Mr. Lewis's next of kin. Notify the security incident response team. Contact Mr. Smith and formally ask that he return the history and physical to the hospital.
d. Arrange for a face-to-face meeting with Mr. Smith to seek return of the history and physical.

Scenario 2

Missing back-up tape

A hospital back-up tape containing unencrypted health information, names, and Social Security numbers of thousands of patients is lost or possibly stolen in delivery to off-site storage. The healthcare organization serves patients across a five-state area, with thousands of victims located in each of the states. In response to this security breach the organization should:

a. Comply with the breach notification regulations of all five states. File a year-end report with the secretary of Health and Human Services.
b. Comply with the breach notification regulations of the state in which healthcare organization is incorporated. Follow federal breach notification regulations by notifying victims and the secretary of Health and Human Services. Do not notify the media.
c. Comply with all applicable federal breach notification requirements only.
d. Comply with the breach notification regulations of all five states. Comply with federal breach notification regulations by notifying the victims, the secretary of Health and Human Services, and major media in each state without unreasonable delay.

Scenario 3

Misdirected e-mail within the network

A clinical laboratory staff member accidently e-mails patient biopsy reports to the office of an urgent care center. The urgent care center is affiliated with the same healthcare network as the clinical laboratory.

The employee of the urgent care center notifies the clinical laboratory supervisor of the misdirected e-mail. The supervisor instructs the employee to delete the e-mail, and the clinical laboratory receives a confirmation that the e-mail was deleted. In response to this misdirected e-mail, the organization should:

a. Do nothing, because the e-mail has been deleted.
b. Send a breach notification to every patients whose biopsy report was in the e-mail.
c. Document the determination that the incident does not represent a significant risk of harm. Do not send a breach notification.
d. Inform both employees that they are under investigation. Suspend the employee responsible for sending the misdirected e-mail pending a further forensic investigation. Seize the computer of the employee receiving the misdirected e-mail and perform an audit for inappropriate activity.

Scenario 4

Patient names disclosed outside the network

A list of clinic patient names is accidentally sent to a physician's office that is not affiliated with the clinic. The list does not include the name of the clinic, or any other identifying information about the patients.

The doctor receiving the misdirected list mails it back to the clinic. No other use or disclosure was made of the list. In response to this incident the clinic should:

a. Do nothing, because the list was returned.
b. Send a breach notification to every patient on the list.
c. Document the determination that the incident does not represent a significant risk of harm. Do not send a breach notification.
d. Because the physician's office viewed the list of patient names they would be required to issue breach notification letters to all individuals on the list.

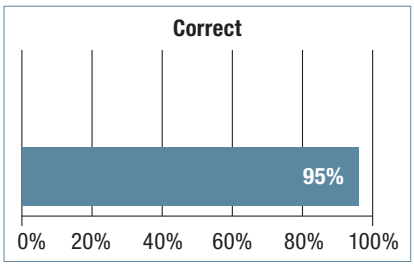
Answers

In December 2009 the *Journal* challenged 500 AHIMA members on the breach notification scenarios. The results are offered here as a benchmark.

Note: The wording of the scenarios presented here has been updated slightly from the December poll; in those instances, greater detail and clarification have been added.

Scenario 1

Inadvertent disclosure of deceased patient information

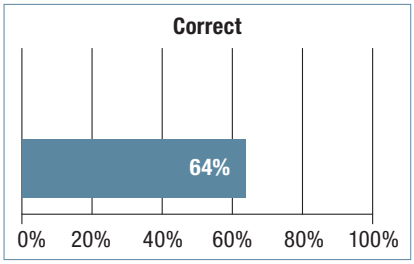


Answer: C. §164.404(d)(1)(ii) of the interim final rule requires that if the individual is deceased, notice must be sent to the last known address of the next of kin or personal representative, if the address is on file.

Commentary from the IFR: "The statute also requires that, if the individual is deceased, notice must be sent to the last known address of the next of kin. The interim final rule adopts this provision at § 164.404(d)(1)(ii), but provides that such notice be sent to either the individual's next of kin or personal representative, as such term is used for purposes of the Privacy Rule, recognizing that in some cases, a covered entity may have contact information for a personal representative of a deceased individual rather than the next of kin. We believe this conforms to the intent of the statute and improves consistency between this subpart and the Privacy Rule. Under 45 CFR 164.502(g), a 'personal representative' of a deceased individual is a person who has authority to act on behalf of the decedent or the decedent's estate. The interim final rule also clarifies that a covered entity is only required to provide notice to next of kin or the personal representative if the covered entity both knows the individual is deceased and has the address of the next of kin or personal representative of the decedent. This clarification should address some of the comments which raised both administrative and privacy concerns with a covered entity being required to obtain contact information for next of kin of a deceased patient, if the individual did not otherwise provide the information while alive." (p.42750)

Scenario 2

Missing back-up tape



Answer: D. Because the breach poses reasonable risk of harm, and because it involves more than 500 people in total, it requires notification of individuals (§164.404)and the HHS secretary (§164.408) without unreasonable delay. Because the breach involves more than 500 people in each state, §164.406 requires notification of major media in each state.
Federal regulations do not preempt state laws, and entities thus must comply with state law as appropriate. Further, entities must comply with laws for those states within which the breach victims reside.

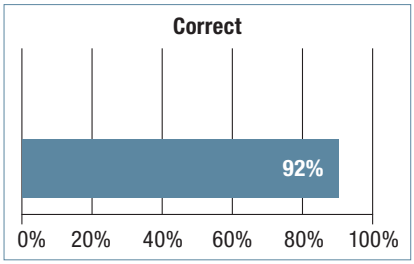
Commentary from the IFR: "In response to comments received, we also offer clarification on how to address a breach involving residents in multiple States or jurisdictions. For example, if a covered entity discovers a breach of 600 individuals, 200 of which reside in Virginia, 200 of which reside in Maryland, and 200 of which reside in the District of Columbia, such a breach did not affect more than 500 residents of any one State or jurisdiction, and as such, notification is not required to be provided to the media pursuant to § 164.406. However, individual notification under § 164.404 would be required, as would notification to the Secretary under § 164.408 because the breach involved 500 or more individuals. Conversely, if a covered entity discovered a breach of unsecured protected health information involving 600 residents within the state of Maryland and 600 residents of the District of Columbia, notification must be provided to a prominent media outlet serving the state of Maryland and to a prominent media outlet serving the District of Columbia." (p. 42752)

"Although we received many comments concerning perceived conflicts between the interaction of State laws and these breach notification provisions, based on the 'contrary' standard for preemption, in general we believe that cov-

ered entities can comply with both the applicable State laws and this regulation. In addition, based on the comments received, we believe that, in most cases, a single notification can satisfy the notification requirements under State laws and this regulation." (p. 42756)

Scenario 3

Misdirected e-mail within network



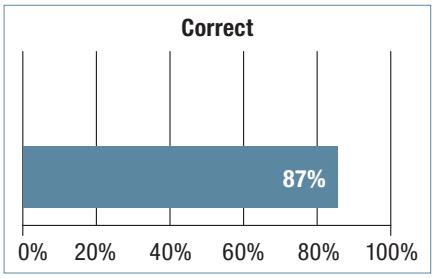
Answer: C. The misdirected e-mail was an unintentional access by a workforce member of the covered entity. It was made in good faith and within the scope of authority, and it did not result in further use or disclosures in a manner not permitted by the privacy rule. The clinical laboratory is responsible for documenting this determination, however.

Commentary from the IFR: "Breach of unsecured protected health information is the acquisition, access, use, or disclosure of PHI in a manner not permitted [by the privacy rule], which compromises the security or privacy of the PHI. Except where:

- unintentional acquisition, access, or use of PHI by workforce member or person acting under authority of CE [covered entity] or BA [business associate], if such acquisition/access/use was made in good faith and within the scope of authority, and does not result in further use of disclosures in a manner not permitted [by the privacy rule];
- Inadvertent disclosure of PHI between persons authorized to access PHI in the same CE or BA, or within the same OHCA, and the information is not further use of disclosed in a manner not permitted [by the privacy rule];
- A disclosure of PHI where a CE/BA has good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain it." (p. 42746)

Scenario 4

Patient names disclosed outside the network



Answer: C. The names on the list are not linked to a healthcare provider, diagnosis, or treatment. Thus no privacy rule violation or security breach resulting in harm to the individuals has occurred. The clinic is responsible for documenting this determination, however.

Commentary from the IFR: "In performing a risk assessment, covered entities and business associates should also consider the type and amount of protected health information involved in the impermissible use or disclosure. If the nature of the protected health information does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach. For example, if a covered entity improperly discloses protected health information that merely included the name of an individual and the fact that he received services from a hospital, then this would constitute a violation of the Privacy Rule, but it may not constitute a significant risk of financial or reputational harm to the individual. In contrast, if the information indicates the type of services that the individual received (such as oncology services), that the individual received services from a specialized facility (such as a substance abuse treatment program 8), or if the protected health information includes information that increases the risk of identity theft (such as a social security number, account number, or mother's maiden name), then there is a higher likelihood that the impermissible use or disclosure compromised the security and privacy of the information." (p. 42745)

Citation

Journal of AHIMA. Web exclusive. February 2010. http://journal.ahima.org. A version of scenario 1 was originally published in the February 2010 print edition.