

HHS Breach Notification Interim Final Rule

Form Your Incident Response Team, Set Policies and Procedures to Comply with New Federal HIPAA Regulations

WHITE PAPER

by Dom Nicastro

The U.S. Department of Health and Human Services (HHS) on August 19 released its interim final rule on breach notification of unsecure protected health information (PHI) and the acceptable methods for covered entities (CE) and business associates (BA) to encrypt and destroy patient records in order to prevent breaches.

HHS published the breach notification rule in the *Federal Register* (45 CFR Parts 160 and 164) August 24.

The American Recovery and Reinvestment Act of 2009 (ARRA) required HHS to issue the final rule six months after President Obama signed into law Title XIII of the ARRA—the Health Information Technology for Clinical and Economic Health (HITECH) Act.

The PHI breach notification regulations took effect September 23. However, HHS will not enforce the rule until February 22, 2010, or thereabouts.

The regulations require:

- Notice to patients alerting them to breaches “without unreasonable delay,” but no later than 60 days after discovery of the breach
- Notice to CEs by BAs when BAs discover a breach
- Notice to the secretary of HHS and prominent media outlets about breaches involving more than 500 patient records
- Notice to next of kin about breaches involving patients who are deceased
- Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the patient, and the CE’s response
- Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records

Experts say CEs and BAs must immediately finalize their breach notification policies and procedures and create an incident response team, regardless of whether the organizations have had major breaches.

FEATURES

- New encryption layers 2
- Harm threshold provision 2
- Anatomy of a breach 3
- Before a breach 4
- During a breach 4
- After a breach 5
- Conclusion 5

“Security breaches happen to the best of companies,” says **Heidi Y. Echols**, partner at McDermott Will & Emery, LLP, in Chicago. “There is only so much you can do to protect against third-party hacking and real legitimate accidents. Things happen. It’s important to start tracking breaches and understand how to respond to them.”

New encryption layers

Some of these encryption layers were not specified in the HHS draft guidance released in April.

- HHS also added encryption layers to specify the technologies and methods that render PHI “unusable, unreadable, or indecipherable to unauthorized individuals.” Some of these layers were not specified in draft guidance released in April.

In the interim final rule, the definitions for acceptable encryption include the following:

- Electronic PHI encrypted as specified in the HIPAA security rule. This includes “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.”
- Valid encryption processes for PHI in databases consistent with National Institute of Standards and Technology (NIST) Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.
- Valid encryption processes for PHI flowing through a network, including wireless, that comply with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*; 800-77, *Guide to IPsec VPNs*; 800-113, *Guide to SSL VPNs*; and others validated by Federal Information Processing Standards 140-2.

The definitions for acceptable destruction include the following:

- Paper, film, or other hard copy media shredded or destroyed so PHI cannot be read or reconstructed. Redaction is specifically excluded as a means of data destruction.
- Electronic media cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*.

“You now need to really consider encryption,” says **Jeff Drummond**, HIPAA blogger and health law partner in the Dallas office of Jackson Walker, LLP. “That’s sort of your first opportunity to avoid breach notification. You can’t do much about your paper records other than destroying them, which eliminates their utility. But for electronic data, you can keep it and use it, but should encrypt so it is considered ‘secured’ under HIPAA.”

Harm threshold provision

In the interim final rule, HHS added a “harm threshold” provision to its definition of a breach. A breach is defined as the “acquisition, access, use, or disclosure of protected health information in a manner not permitted under

[the privacy rule] which compromises the security or privacy of the protected health information.”

HHS clarified in the interim final rule that in order for breach notification to be triggered, the PHI disclosed must pose a “significant risk of financial, reputational, or other harm to the individual.”

Conduct a risk assessment to determine whether there is significant risk of harm to the individual.

● CEs and BAs must perform a risk assessment to determine whether there is significant risk of harm to the individual whose PHI was inappropriately dispensed into the wrong hands.

According to the interim final rule, CEs and BAs should ask the following important questions to determine whether the breach meets the harm threshold:

- In whose hands did the PHI land?
- Can the information disclosed cause “significant risk of financial, reputational, or other harm to the individual”?
- Was mitigation possible? For example, can you obtain forensic proof that a stolen laptop computer’s data were not accessed?

“The harm threshold is something that’s quite a bit different,” says **Rebecca Herold, CISSP, CIPP, CISM, CISA, FLMI**. Herold serves as privacy, security, and compliance consultant at Rebecca Herold & Associates, LLC, in Des Moines, IA, and provides a HIPAA/HITECH Act compliance tool at www.compliancehelper.com. “That’s caused a lot of debate from privacy advocates because they worry there will be a tendency for covered entities and business associates to say, ‘Well, a breach happened, but it’s not likely anything bad will happen,’” she says.

Herold hopes HHS will provide more specific guidelines for steps CEs and BAs should take to make a determination of harm to individuals.

“Right now, there’s not a good set of directions, but I anticipate some guidance documents will be released by HHS prior to the February compliance date,” she says.

HHS’ guidance in the interim final rule calls for CEs and BAs to “consider who impermissibly used or to whom the information was impermissibly disclosed when evaluating the risk of harm to individuals.”

Anatomy of a breach: Before, during, and after

Although CEs and BAs should have breach notification policies in place, they must also know how to prevent breaches.

“You don’t get to the HITECH until you have a privacy breach,” says **Andrew E. Blustein, Esq.**, partner and cochair of Garfunkel, Wild & Travis’ Health Information and Technology Group in Great Neck, NY; Hackensack, NJ; and

Stamford, CT. "If you have good things in your privacy program, you should never get to it."

Consider Blustein's tips for how to respond to a breach before, during, and after it happens.

Before

- **Establish appropriate technical safeguards to protect patient information.** Require encryption for laptops and other portable devices. Establish remote access roles specific to applications and business requirements. Prohibit the installation of unsecured "home-made" software on laptops. Develop policies regarding the protection of patient information transmitted from remote locations.
- **Discuss with vendors their responsibility for protecting patient information.** Vendors who are BAs must enter into an agreement with the CE. Further, contact each of your vendors and discuss appropriate safeguards to protect your PHI. If your BA is an agent of the CE, the CE is considered to have notice of the breach at the time the BA has notice. Make clear the lines of communication and responsibility between you and your BA.
- **Perform routine audits of employee access to PHI.** Let employees know you are conducting the audits. Inform them that you intend for the audits to revitalize the organization's policy.
- **Establish a security incident response team.** Assign an individual to be responsible for organizing responses to security incidents. Appoint a core team to conduct the investigation (e.g., representatives from IT, HR, risk management, legal, and security departments). Include technical and administrative staff members, as well as staff members directly involved in the incident. "You can't do this on the fly," Blustein says. Build your team carefully and conduct mock breaches.
- **Prepare written policies that address the process for internal reporting.** Consider what potential breaches need to be reported internally and to whom individuals should report these violations. Set time frames for reporting. "In some cases, you don't want to wait for the investigation team's full report," Blustein says. "Sometimes you want a flash report." Educate staff members and publicize an actual breach in the organization as a teaching moment. Don't keep it quiet.

Don't keep the breach quiet. Publicize it. Use it as a teaching moment.

During

- **Initiate an investigation immediately.** The team leader, or point person, must be ready for action. Immediately consider whether the organization needs to make a report to authorities. Ask the following questions:
 - What information was potentially disclosed?
 - What technical safeguards were in place?

- How many people were affected?
- Could the information be used adversely against such individuals?

- **Determine whether an exception to the notification requirement applies.** Was the breach such that the person receiving the information would not be able to retain and use it? Was it an unintentional disclosure in good faith or an inadvertent disclosure to another individual at the same facility?
- **Determine the need to notify the individual.** Check the regulations contained in the HHS interim final rule and state breach notification laws. Consider whether notification could mitigate any harmful effects on the individual. If a patient's credit card or Social Security information was stolen, it may be appropriate to offer them credit monitoring services, Blustein says.
- **Determine appropriate sanctions.** Following through on appropriate internal sanctions can send a chilling message throughout your organization, Blustein says. "Also, if [the Office for Civil Rights] comes in, and something egregious occurred and you've done nothing about it, what are you doing about mitigating the problem in the future?" he says. Depending on the employee involved and the type of violation, consider offering additional HIPAA training, issuing a warning, putting the employee on probation or suspension, or, in extreme situations, terminating the employee.

Consider offering additional HIPAA training for those who commit a breach.

After

Below are eight final checklist items to conduct once your team responds accordingly to a breach:

- Incorporate lessons learned into existing procedures (were internal reporting and investigation fast and efficient?)
- Include the breach on the annual log reported to HHS
- Modify policies as necessary
- Reeducate staff members regarding lessons learned
- Look for repeating patterns (e.g., one patient area that has multiple incidents)
- Include the unauthorized disclosure on the accounting of disclosures
- Include any sanctions on the HIPAA sanctions log
- Ensure that investigation notes and reports were appropriately detailed and that they are maintained

Conclusion

HHS says it will not enforce breach notification provisions until February 2010—or 180 days from the publication of the interim final rule—but HITECH states that CEs are subject now to penalties for noncompliance.

CEs should have breach response systems in place already, says **Chris Simons, RHIA**, director of UM and HIM and the privacy officer at Spring Harbor Hospital in Westbrook, ME.

However, if CEs still need to work on their policies, they should focus their energies on making sure staff members understand the process for and importance of prompt reporting.

“If your staff doesn’t know who their privacy officer is, that’s a problem,” Simons says. “That’s a good starting place. Make sure staff knows what a breach is and who to report it to. They should be encouraged to immediately report even the suspicion of an issue.”

A risk analysis could help you prevent a breach in the first place.

- Document everything your organization does in response to a suspected breach, Simons adds. Conduct a risk analysis to expose your internal weaknesses. It could help you prevent a breach in the first place, which, after all, is the goal.

“What are your serious risks, and what are your minor risks?” Simons says. “How are you educating people, and are your policies and procedures in place? Get out there and do your rounds to see what’s going on and see if you hear things.”

Sources: HHS’ “Breach Notification for Unsecured Protected Health Information; Interim Final Rule;” and the HITECH Act.