Time for a HIPAA Tune-Up?: Penalties Now in Effect for Noncompliance

by Carol Ann Quinsey, RHIA, CHPS

On February 16, 2006, the Department of Health and Human Services published the final rule adopting policies enforcing the HIPAA provisions. The rule imposes civil monetary penalties on covered entities that violate any of the HIPAA administrative simplification rules, not just the privacy rule.[1] Effective March 16, 2006, the rule follows enforcement from the time a complaint is filed through investigation to conclusion.

Given this announcement, now is a good time for organizations to review their compliance efforts and tune them up as necessary.

Bad News Makes Good News

It may seem that some states or areas of the country have more problems with privacy and security breaches than others. However, this may be a matter of publicity. Some states such as California have legislated public disclosure of such breaches, whereas providers in other states may not be required to make the public aware of breaches.

Overall, by mid-2005 the Office for Civil Rights had received nearly 14,000 complaints alleging privacy rule violations. Approximately two-thirds of the complaints had been resolved, and one-third were still under investigation. A very small percentage had been referred to the Department of Justice for criminal investigation.[2]

Privacy and security breaches continue to make headlines. For example, Providence Healthcare disclosed that in December 2005 approximately 365,000 medical records of hospice and home health patients were lost when backup computer tapes and disks were stolen from a parked car in Portland, OR. The healthcare provider has since implemented solutions to make its data more secure and notified affected patients by mail about the theft. To date, there have been no verified reports that the stolen data have been used illegally.[3]

Compliance Checklist

Every organization should verify that its policies and procedures support full HIPAA compliance and that practice in the facility follows those policies and procedures. HIM professionals should walk through their facilities using the following checklist to ensure the privacy and security of their patients' information.

Oral Disclosures

- Are staff discussions held in areas where conversations are not easily overheard?
- Are conversations with patients and family members held in areas where personal health information (PHI) is not easily overheard?
- Do phone conversations, dictation, and conversations on speakerphones take place in areas where PHI is not easily overheard?
- Are doors to exam or patient rooms closed when discussing PHI?
- Is only the minimum amount of PHI overheard in waiting rooms?

Privacy Safeguards

- Are computer screens and monitors positioned so information cannot be viewed inappropriately?

- Are doors to nonpublic areas kept shut?
- Are documents, films, or other media containing PHI concealed from public access and view?
- Are white boards placed in discreet locations?
- Do white boards contain the minimum necessary PHI to allow staff to do their jobs easily and safely?
- Is PHI stored or filed in secure locations, away from public access and view?
- Do sign-in sheets include the minimum necessary PHI?
- Are copiers and fax machines attended or located in secure areas away from public access?
- Are patient rosters or lists kept out of public view and access?
- Are notices of privacy practices posted in appropriate locations?
- Do registration personnel ask appropriate questions about inclusion in the facility directory?

Staff Conduct

- Do staff members know how to handle requests from patients about their health information (e.g., how to access, amend, or request restrictions)?
- Can staff identify how and to whom privacy-related concerns or complaints should be directed?
- Is PHI disposed of properly throughout the facility (e.g., placed in secure document disposal containers)?[4]

Security Safeguards

- Are passwords assigned and used by staff appropriately (e.g., uniquely assigned and never shared)?
- Do computer systems produce audit trails, and are such documents routinely monitored for compliance with policies and procedures?
- Is there adequate redundancy and backup for mission-critical computer systems so clinical information is available when needed to provide patient care?
- Have there been tests to ensure that data can be restored in the event of a crash?
- Is there a plan for failover, so that if one server fails, activity transfers smoothly to another? Is there backup power supply?
- Is there an adequate balance of protection for PHI that still allows healthcare providers to do their jobs?
- Can staff state what a security incident is and where to report any security incidents?
- Has staff training been an ongoing function, with periodic reminders and updates about malicious spyware or viruses and how to select strong passwords?
- Have games or other inappropriate software been downloaded to computers attached to the network, or are downloads otherwise out of step with policies?
- Are there processes to ensure that users have strong passwords, do not share them, and are not exchanging PHI in e-mail?

Using the above questions as a start, organizations can create a checklist to verify that they remain in compliance with the HIPAA privacy and security rules. Many large healthcare facilities created extensive checklists as part of their original HIPAA implementations. Revisit these documents and give them new life by documenting continuing adherence to policies and procedures that were implemented previously.

A HIPAA walkthrough can reveal that policies and procedures need to be modified, shine a light on training issues that need attention, or yield evidence that the organization is in compliance with HIPAA administrative simplification rules. Conducting a walkthrough is just part of the ongoing due diligence called for in the rules. Organizations that are simply responding to complaints have a long way to go to ensure full HIPAA compliance.

In the wake of Hurricane Katrina, the importance of adequate backup protection for health information became crystal clear. While these losses may not result in HIPAA complaints being filed, they do provide an additional impetus to add the backup provisions in the HIPAA security rule as part of a HIPAA tune up.

Notes

1. "HIPAA Administration Simplification: Enforcement; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 71, no. 32 (2006). Available online at www.gpoaccess.gov/fr.
2. HCPro. "In the News." *Briefings* on HIPAA 5, no. 9 (2005). Available online at www.hcpro.com.
3. Weiss, Todd. "Four Lose Jobs after Data Breach at Oregon Health Care Facility." *ComputerWorld*, February 28, 2006. Available online at www.computerworld.com.
4. Good Samaritan Hospital, Vincennes, IN. "Privacy/Security Walkthrough Checklist." Abstracted with permission. Available online in the AHIMA HIPAA Community of Practice at www.ahima.org.

Reference

Walsh, Tom. "The 26.2-mile Security Rule." *Journal of AHIMA* 76, no. 3 (2005): 24-27. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.

Acknowledgments

Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS
Beth Hjort, RHIA, CHP
Wendy M. Mangin, MS, RHIA
Lydia Washington, MS, RHIA, CPHIMS

Carol Ann Quinsey *(carol.quinsey@ahima.org) is a professional practice manager at AHIMA.*

Article citation:
Quinsey, Carol Ann. "Time for a HIPAA Tune-Up?: Penalties Now in Effect for Noncompliance" *Journal of AHIMA* 77, no.5 (May 2006): 64-65.