Sorting Out Employee Sanctions

by Jill Burrington-Brown, MS, RHIA

Has your organization addressed sanctions related to privacy and security issues? Both the final privacy rule and final security rule address this issue. The privacy rule states that the covered entity must "have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity," and the security rule states relatively the same thing. Every covered entity must have policies and procedures that address:

- appropriate employee behavior regarding privacy and security
- typical sanctions for noncompliance of the policies and procedures
- communication to and education of the work force
- the sanction application process (investigations and terminations)

The covered entity should develop privacy and security sanction policies with the involvement of all interested stakeholders such as privacy and security officers, executives, and the human resources, quality improvement, risk management, and HIM departments. Using their expertise and existing policies will ensure a more successful implementation of your program. This article will explain how to implement an employee compliance and sanction program.

Start with the Basics

What does the employee need to know about privacy and security? The best way to deliver the message is to explain it as simply as possible:

- privacy is important
- medical information is confidential
- there are specific times when you may share what you know

Certainly those of us in HIM already understand this, but the audience will be broad and include personnel who may not be familiar with basic HIM notions about security and privacy of patient health information. Explaining the above concepts through the use of scenarios (both real and fictional) will help explain the breadth and depth of the issue.

Spell out Sanctions

Employees must be informed of the disciplinary actions the covered entity will take in the event of a privacy or security incident. This must also include giving notice of the possible civil and criminal penalties for misuse or misappropriation of health information.

Sanctions might include verbal warnings, removal of system privileges, and termination of employment. Organizations will want to consider the range of disciplinary actions, from verbal or written warnings to termination of employment, and match them to the types of infractions. For example, violations that are inadvertent, of low severity, and indicate a need for training may only require verbal correction and retraining. Such violations might be clinician conversations in semi-public areas or delivery of health records to the wrong clinical area.

Deliberate, intentional infractions should trigger a disciplinary process that results in termination of employment. These types of infractions might include the sale of confidential information or the unauthorized access of health information out of curiosity. Whatever the infractions, covered entities must make every effort to apply the sanctions evenly across all job classes in order to avoid actions that might lead to employment discrimination charges.

Make Time for Training

Educating staff is the next step in building a reasonable compliance and sanction program. The covered entity should provide and document privacy training to all staff as is appropriate to their job duties. The organization should include not only the policies regarding protected health information (PHI) but also the consequences of both inadvertent and deliberate violations of PHI policies.

The covered entity should document that staff training was provided. It should also have each member sign a confidentiality agreement indicating understanding of the policies and the possible repercussions of any type of security or privacy incident.

Investigating Violations

Organizations must address the process of investigation. While the privacy rule specifies that a privacy officer must be appointed and be responsible about the development and implementation of policies and procedures, this does not mean the privacy officer is responsible for the roles traditionally fulfilled by human resources. In fact, the privacy officer must work through the complaint, investigation, and employee sanction process with human resources to make sure all other applicable employment laws and union regulations are followed.

It is also important to note that the privacy officer may not need to be involved in all employee actions if the policies and procedures are detailed and thorough. Finally, if sanctions are applied in any disciplinary process, they must be documented.

Many healthcare organizations include volunteers and credentialed healthcare staff in their work force. Because this part of the work force is not controlled by employment, the sanction process must be carefully considered in order to be appropriately and fairly applied.

The sanctions for minor, inadvertent infractions can be quite similar to those for the employed work force. However, job suspensions and terminations are more difficult with volunteers and physicians who are not hired. Asking the volunteer not to return does not seem as severe a consequence as job termination, but it may be what the organization decides is appropriate.

A physician who has gone through an extensive credentialing process will likely have the medical staff bylaws to follow. These bylaws should be reviewed for compliance with the rules and to establish a process for physician infractions requiring more severe consequences than retraining.

Members of an organization's work force will better understand the need for privacy and security policies when they understand that the civil and criminal penalties for violations of the rules are stiff. Civil fines can amount to $25,000 for repeated violations in the same year, and the deliberate misuse of PHI can incur a $250,000 fine along with 10 years imprisonment.

References

Arnall Golden Gregory LLP. "Privacy Rule Takes Effect April 14, 2001: The Clock is Ticking." *HIPAA Bulletin*. May 2001. Available at www.agg.com/Publications/Healthcare-HIPAABulletin-0501-2.html.

Opus Communications. "Develop Employee Sanctions for Privacy Violations." *Briefings on HIPAA* 2, no. 7 (2002): 1-3.

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 67, no. 157 (August 14, 2002). Available at http://aspe.hhs.gov/ admnsimp/.

Jill Burrington-Brown *(jill.burrington-brown@ahima.org) is an HIM practice manager at AHIMA.*

Article citation:
Burrington-Brown, Jill. "Sorting out Employee Sanctions." *Journal of AHIMA* 74, no.6 (June 2003): 53-54.