First Line of Defense Against Privacy Complaints (HIPAA on the Job)

by Margret Amatayakul, RHIA, FHIMSS

Every healthcare provider has experienced managing patient complaints, whether they are about cold food, unresponsive staff, or missed medication. However, when it comes to privacy and confidentiality, complaints need to be handled a bit differently. In this article, we'll explore how to handle privacy complaints under HIPAA.

The notice of privacy practices given to individuals must include information about filing complaints with both the covered entity and the secretary of the US Department of Health and Human Services (HHS). In addition to the notice, any denial of access or amendment must be accompanied by information on how to file a complaint with the covered entity and the secretary. The privacy rule does not limit the opportunity to file complaints to patients or health plan enrollees, therefore permitting members of the work force, oversight bodies such as state health departments or the Joint Commission, and the public to file a complaint.

A Careful Response Is Key

A covered entity should make every effort to encourage potential complainants to first address their complaints to the entity itself. The covered entity should make it easy to file a complaint and be highly responsive. For example, the employee responsible for receiving privacy complaints should have a pleasant demeanor and proper training in how to respond to such complaints. Further, forms on which to record complaints should be designed to promote goodwill and invite ideas for improvement. Regardless of how the complaint is received, the organization should stress the importance it places on privacy and its receptivity to learning about privacy concerns. To demonstrate HIPAA compliance, ask for the complaint in writing or document the complaint when it is received.

Every identifiable complaint should generate an investigation and a response. The investigation should focus on both the specific complaint and any patterns of similar complaints. It is helpful to coordinate privacy complaints with security incidents to determine potential causal relationships. If after an investigation it is determined that no actual violation occurred, the covered entity should recognize that perception of a violation is as important as an actual violation and may need to take corrective action steps to overcome erroneous perceptions.

The organization should respond to every identifiable complaint received. If the complaint was filed in person or on the phone, it should be documented and followed with a phone call or letter. The response should include a statement of appreciation for the individual's value as a patient/customer and a recognition of the time and interest taken in advising the covered entity of the privacy concern.

The privacy response should be made promptly and include information about measures being taken to continuously improve privacy practices. Exercise care in acknowledging an actual privacy violation and in describing any new procedures implemented. Privacy is a very personal matter and can therefore be a very ambiguous area to address. What one individual may consider an invasion of privacy or violation of privacy rights may not be a violation to another individual. Keep in mind that the passage of time may change perceptions as well. Finally, if an investigation reveals an actual violation, it is best to involve risk management and legal counsel in drafting the response that best suits the situation, including any offer of mitigation.

Complaints Can Yield HHS Investigations

The greatest potential impact of the privacy complaint requirement is that a complaint filed with HHS may result in an investigation of the covered entity. Although the promised enforcement regulation has not yet been published, the privacy rule specifies the secretary's investigative authority. Further, any investigation is likely to include all matters of HIPAA privacy, not

just that which triggered the investigation. Because HIPAA is an unfunded mandate, it is likely that the only way a covered entity will be investigated is upon the filing of a complaint. Although the compliance date is months off and HHS has not yet published procedures for the filing of complaints, the agency has indicated that privacy complaints have already been filed by the public.

An investigation requires the covered entity to supply a compliance report and documentation of its privacy practices. It must demonstrate that it has privacy policies and procedures and members of its work force have been trained. The contents of the compliance report are not specified, but covered entities would be advised to ensure they monitor compliance and document findings and corrective action.

A simple spreadsheet or database can be used as an index to policies and procedures as they relate to the HIPAA privacy standards and to catalog training. This same tool can be used to tally privacy complaints against standards and to record the organization's own assessment (see "Privacy and Security Event Log" below). Although the healthcare industry is currently focused on becoming HIPAA compliant, constant vigilance and an ongoing compliance monitoring plan will be needed to ensure that new policies, practices, or technologies support continuous improvement.

An Opportunity for Consolidation

Planning the provision of the notice on filing a privacy complaint and how to provide an appropriate response also presents an opportunity to coordinate a process that has become fragmented and resource-intensive in many organizations. As a result of many different regulations and accreditation initiatives, healthcare providers have added measures like corporate compliance hotlines, sentinel event reporting, patient satisfaction surveys, and patient relations/customer service activities to their existing incident reporting mechanisms, risk management, and quality improvement activities. HIPAA adds privacy complaint collection and security incident reporting.

Many providers are recognizing this situation as an opportunity to revamp and potentially consolidate these activities. Multiple independent reporting mechanisms can be confusing and may result in lack of appropriate reporting simply because it is not clear to whom an event should be reported. Further, detecting violation patterns may be more difficult if complaints are captured through different systems.

Consider the following options for collecting and tracking privacy complaints:

- **centralize reporting**, with respective areas analyzing the events for appropriate action. Software used in the information technology department's help desk could be used for receiving and tracking all issues and their resolution, while the actual investigation and corrective action is taking place in the separate departments of risk management, compliance, etc.
- **set up individual reporting mechanisms** and "first line of defense" in the respective departments, but consolidating results at the back end for quality improvement
- **centralize all functions** with a single point of contact, resolution, and reporting

HIPAA has become the driving force behind consolidating privacy policies and procedures because privacy cuts across all disciplines and organizational boundaries. In fact, it may be the catalyst needed to address many other areas needing greater coordination. A good way to begin an organizational assessment is by creating a flowchart of all potential points of complaint contact and how each follows through to resolution and reporting. If the organization chooses to retain multiple points of collection, the flowchart may be useful in explaining to the work force what issues are addressed where and how they get resolved.

privacy complaint tool box

In preparation for complaints, create a privacy complaint "tool box" comprised of the following items: ___ privacy office ___ designated personnel trained in customer service ___ issue collection and resolution flowchart	___ response/follow-up call script ___ response/follow-up letter template ___ complaint and incident pattern analysis ___ issue resolution log ___ continuous monitoring plan ___ periodic independent verification and

___ privacy complaint collection form ___ security incident reporting form ___ complaint and incident log	validation ___ triggered reviews ___ feedback mechanism ___ management report

privacy and security event log

Standard	Related Policies and Procedures	Training		Number and Description of Events	Owner	Resolution	Follow Up
		All	Target				
Notice of privacy practices	Policy and procedure for provision of notice & acknowledg-ment of receipt	Annual	Admitting/ registration	3--Lack of understanding 1--Non-receipt	Corporate compliance Admitting/ registration	Added summary to acknowledg-ment form Retrained admitting/ registration staff	Patient satisfaction survey

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "The First Line of Defense Against Privacy Complaints (HIPAA on the Job series)." *Journal of AHIMA* 73, no.9 (2002): 24A-C.