

HIPAA Whistleblower Protections Promote Information Governance

Save to myBoK

By Mary Butler

Health information management (HIM) professionals are too often witness to an array of fraudulent activities, whether its fraud via “upcoding,” improper disclosure of protected health information (PHI), or other breach activities.

Since reporting noncompliance could require potential whistleblowers to provide evidence of abuses (which may or may not require disclosing PHI), they are often discouraged from coming forward. And even though there are federal laws to protect individuals from whistleblower retaliation, workforce members and the organizations that employ them can pay an emotional or financial price even if a formal investigation clears them of any wrongdoing.

However, a new, frequently overlooked provision of the [HITECH-HIPAA Omnibus Final Rule](#) permits workforce member disclosures of PHI to proper oversight authorities provided that: “The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public...” (See section [164.502 of the Final Rule](#)).

When this rule was in its preliminary phases, commenters objected to this provision, arguing that the rules protecting individual whistleblowers were adequate, and thus asked that it be stripped from the law.

But the terms of the Final Rule dismissed this request, noting that “Our purpose in including this provision is to make clear that we are not erecting a new barrier to whistleblowing, and that covered entities may not use this rule as a mechanism for sanctioning workforce members or business associates for whistleblowing activity.” It continues, “Whistleblowers, by their unique insider position, have access to critical information not otherwise easily attainable by oversight and enforcement organizations.”

Changing Perception of ‘Whistleblowers’

According to Kim Baldwin Stried-Reich, MBA, MJ, PBCI, RHIA, CPHQ, FAHIMA, the former Speaker of the AHIMA House of Delegates, the new amendment to the HITECH-HIPAA Omnibus rule demonstrates both the increasing importance and value HIM professionals have today in ensuring both integrity and compliance with rules, regulations, and laws governing access and disclosure of health information within their organizations. Baldwin Stried-Reich is a privacy and compliance officer with the Lake County Physicians Association, in Waukegan, IL.

She notes that while the new provision provides specific protections against disclosures reported to an oversight agency by whistleblowers and workforce members who are victims of a crime, she’s not so sure this new rule will encourage individuals, such as HIM professionals to speak-up and speak-out when or if they see evidence of systematic and ongoing non-compliance with federal mandates.

One reason for this is the widespread use of the word “whistleblower,” which often carries negative connotations. She prefers the term “corporate integrity advocate.”

“Perhaps if Health and Human Services had utilized another term, such as ‘corporate integrity advocate’ more individuals would understand what the intent of this new law is and that it is meant as an avenue individuals can choose to pursue if their professional integrity and ethics are not in alignment with the corporation’s any longer,” Baldwin Stried-Reich says.

A relevant example of this is evident [in the settlement](#) that [Shasta Regional Medical Center \(SRMC\)](#) entered into with the Department of Health and Human Services (HHS) following an investigation concerning the breach of PHI after senior-level executives intentionally disclosed protected information to the media on at least three separate occasions.

The Shasta case demonstrates how and why corporate integrity advocates or whistleblowers are needed to facilitate change within their organizations when it is warranted, Baldwin Stried-Reich explains.

HITECH-HIPAA and Information Governance

The provision protects covered entities from significant fines and penalties from HHS's Office for Civil Rights in the event a whistleblower's accusations are determined to be unfounded. Or if, for example, an alleged whistleblower is a disgruntled employee. This rule is a step in the right direction for HIM professionals because it encourages them to maintain the integrity of the records they oversee and because it demands improved information governance, she says.

"The best protection an organization can—and should—do to protect against a HIPAA whistleblowing claim is to establish sound information governance programs within their organizations. That includes education, training, policies and procedures and an ongoing review of internal controls as well as all mobile devices and biomedical applications in use," Baldwin-Stried Reich says.

"Whistleblowing is never a good first option, nor is it a shield or protection, it should be utilized when an individual believes in good faith that rules are being broken and he or she has no other option but to bring his or her claims forward," she adds.

It is this type of workforce member activity that exemplifies Baldwin Stried-Reich's preference for the term "corporate integrity advocate."

To that end, the rule stipulates that such a disclosure should be made to "a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity," or "an attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options..."

Baldwin-Stried Reich says these new protections aren't very well understood yet by the industry, though it will become increasingly important as organizations become involved in information governance programs. And if covered entities aren't familiar with these protections—or even best practices for good information governance, they are putting themselves at risk for security and privacy breaches that the OCR now has more latitude to enforce.

According to a recent report by [Redspin](#), since the enactment of the HITECH breach reporting requirement, there have been a total of 804 large-scale breaches of PHI affecting over 29.2 million patient records, with 22.1 percent of these breaches resulting from unauthorized access and another 35 percent of the incidents due to the loss or theft of an unencrypted laptop or other mobile electronic device.

Preventing Whistleblower Scenarios

The best way for a covered entity to avoid whistleblower disclosures is to have excellent privacy and security practices in place, both of which demonstrate sound information governance. This is particularly important for covered entities as e-discovery investigations become more prevalent in an increasingly EHR world.

Baldwin Stried-Reich says the best way to start is through education programs—make sure workforce members are aware of the whistleblower provisions of HIPAA as part of compliance training. Entities should then look at privacy and security basics such as data encryption, tracking how data flows in and out of an organization, conducting data mapping, and making sure the doors are locked to rooms that store data.

Baldwin Stried-Reich says this regulation is an opportunity for HIM professionals, "It's a way of saying there's a needed role in our profession in terms of information integrity and the role we have in information governance and what we do to add value to the process."

Mary Butler (mary.butler@ahima.org) is the associate editor at the Journal of AHIMA.

Original source:

Butler, Mary. "HIPAA Whistleblower Protections Promote Information Governance" ([Journal of AHIMA website](#)), March 01, 2014.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.