Codify
BY AAPC

Health Information Compliance Alert

Security: With Sanctions Policies, 'Shame On You' Just Won't Do

From warnings to termination, you must show determination

Like a strict nun packing a sturdy ruler, your facility must be equipped with a sanctions policy in case any of your employees violate any portion of HIPAA. Not having such a policy in place means you're not only giving potentially harmful employees free rein to make damaging HIPAA abuses - you're also breaking the law.

According to the reg, "a 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 ..." That doesn't mean you have to spell out what disciplinary actions you'll take for HIPAA non-compliance, but it does require you to create - and make available for employees - your own policy.

But for an environment in which potential violations could run the gamut from minor to extreme, should disciplinary actions be spelled out? Yes, say many HIPAA experts - but only when specificity is feasible.

"[Some] people set up their privacy rule violations on a grade where it's unintentional versus intentional," says **Robert Markette**, an attorney with **Gilliland & Caudill** in Indianapolis. Markette advises facilities to include the types of potential violations in their policies and procedures and to include in what manner employees would be disciplined in specific situations. "Obviously you'll have to improvise when something unanticipated comes up, but you need to put the employees on notice [about the most egregious violations]," he says.

While you may have to "improvise" when it comes to sanctioning an employee for a HIPAA breach, what's more critical is to make sure staff knows there are consequences for improper disclosures and other HIPAA violations. "If staff doesn't really believe there are going to be any consequences [for HIPAA breaches], then we're doomed," notes **Patricia Johnston**, a consultant with **Texas Health Resources** in Arlington. Johnston says she makes an effort not to focus on the negative, but says employees must be reminded that there are consequences for non-compliance with the facility's policies that can include termination.

Johnston tells **Eli** she's broken down THR's sanctions policy into three levels of non-compliance: 1) carelessness; 2) curiosity; and 3) maliciousness, willfulness or non-compliance for personal gain. Here's an example of each level:

Level 1: An employee faxes PHI to the wrong location. This happens all the time at many facilities, says Johnston.

Level 2: An employee knows he probably shouldn't be looking at a document or computer file he shouldn't have access to, but does so anyway. For example, the employee may recognize a patient as a neighbor and could take a peek at the latter's chart.

Level 3: An employee willfully and maliciously obtains PHI for the purpose of selling the data or to defame someone. There's obvious harm intended in this situation.

Johnston says the first two levels allow for latitude as far as the types of sanctions the employee may face; they could range from simple re-training all the way to termination, but disciplinary actions will depend on the situation, the fact pattern and if there have been trends or a series of incidents. As for the third level - that results in termination. "There really isn't any latitude with [level 3]," she insists.

As far as who reviews any sanctionable offenses, your privacy officer should be heavily involved in the process, but also include other officials whenever appropriate, such as in-house counsel or other senior management - especially for

egregious violations, says **Brian Gradle**, an attorney with **Hogan & Hartson** in Washington.

Gradle advises facilities first to take appropriate steps to mediate any harm that's been caused by the disclosure and then consider what sanctions, if any, are appropriate in that specific situation. If an employee had made inappropriate disclosures that occurred three or four years ago - before HIPAA went into effect - that may establish a precedent and help you determine the appropriate punishment.

Yet Gradle admits that many facilities simply don't have a clear-cut gradation for the severity of offenses and what punishments will be applied. As he notes, "there just isn't five yards for holding and ten for intentional grounding." You'll have to contemplate what type of offense calls for what punishment. Just make sure your staff knows there are consequences for inappropriate disclosures of confidential data.