Health Information Compliance Alert

PRIVACY COMPLIANCE ~ 8 Questions To Ask When Drafting HIPAA Sanction Policies

Have you recently taken a look at your list of what constitutes a violation of the privacy rule within your organization? If not, your privacy rule sanction policies may need tightening or rethinking

Rule review: The Health Insurance Portability and Accountability Act privacy requirements mandate that all covered entities "develop and apply when appropriate sanctions for failure to comply with policies or procedures of the covered entity" or with the requirements of the NPRM.

Anyone who has regular contact with protected health information is subject to sanctions, as well as the covered entity's business partners.

Covered entities must develop and impose sanctions "appropriate to the nature of the issue."

Types of sanctions that may be applied would vary according to factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicates a "pattern or practice of improper use or disclosure" of PHI.

One size does not fit all: The **Department of Health and Human Services** noted in the rule it had considered specifying particular sanctions for specific violations of privacy policy but had abandoned that approach because "we cannot anticipate every kind of privacy policy issue in advance, [and] we cannot predict the response that would be appropriate" for each violation.

Bill Sarraille, an attorney with Arent Fox Kintner Plotkin & Kahn, says there are several important questions privacy officers should ask themselves when drumming up ideas for potential sanctions:

- **How egregious is the violation itself?** One man's misdemeanor is another's blatant transgression. Come up with a system that indicates the severity of any given violation.

- **How intentional or unintentional was the violation?** Answering this question is naturally subjective, but privacy officers should be able to gauge the level of intent, says Sarraille.

- **How great was the harm?**

- **How fixable is the harm?**

- **Has the person in violation of the rules taken responsibility for his or her actions?** Also, has the person cooperated in the investigation and in ameliorating the problem, to the extent that the problem could be fixed?

- **How clearly was the person who made the violation put on notice about the issue?**

- **Is the proposed sanction consistent with what you've done in other circumstances?**

Sarraille tells **Eli** there are a host of other considerations that must be made in order to remain vigilant and yet equitable with employees who violate HIPAA. He believes the facts and circumstances of the infraction will dictate the level of punishment.

But since there's a level of subjectivity involved in the process, Sarraille says the last question noted above is crucial for privacy officers to ask themselves, since it's easy to let people's standing in the organization or their economic importance to the company affect one's objective assessment.

Doing that would undermine the credibility of what you've done by way of discipline, he warns: "If there's one standard for the higher-ups and another for the lower-down-the-line folks, that immediately reads to the organization as a whole, and the entire compliance process is dismissed cynically."

And as far as who should be creating the list of sanctions, Sarraille believes in a group effort consisting of a privacy officer and human resources officials. A privacy committee, if one exists in your institution, should review the proposals before they're put in print, he advises.