Health Information Compliance Alert

HIPAA Privacy: DON'T GIVE GRIEF RECEIVE IT

If a health care provider has already created and implemented a fraud and abuse compliance program, then developing a grievance policy for HIPAA-related complaints is only a hop, skip and a jump away.

According to the **Department of Health and Human Services'** Health Insurance Portability and Accountability Act privacy rule, part of a covered entity's responsibilities to ensure the confidentiality of protected health information necessitates the implementation of a grievance policy, or a "means for patients to make inquiries or complaints regarding the privacy of their records."

HIPAA-related complaints can be made by anyone, not simply by an aggrieved person, and there can't be any retaliation against anyone who makes a complaint, according to **Bill Sarraille**, an attorney with the Washington office of **Arent Fox**.

Sarraille says the information on how to make a complaint, both internally and to the **HHS Office for Civil Rights**, needs to be in the notice of privacy practices. He says it makes sense for providers to make the internal complaint process as easy internally as possible in order to help convince people with issues that that complaining internally is better and easier than turning to the OCR.

Creating a grievance policy isn't as difficult as it may appear initially, but it involves several steps:

1. **No need to duplicate an existing office.** For the most part, if a provider already has a fraud and abuse complaint officer staffed, then that person should also be responsible for fielding HIPAA-related complaints. Sarraille says the best person for the job is usually the privacy officer. The privacy officer would also interpret the complaints and determine the consequences of the complaint in terms of the privacy standards.

2. **Assign a reasonable person for the job.** There's certainly no sense in hiring someone to field complaints who's insensitive, combative or generally hostile, Sarraille asserts. It's appropriate to find someone who can communicate and perform well with irate people.

   "It's basically a matter of being a good listener, of not being defensive, of assuring people in the contexts of those kinds of communications that there is a commitment to safeguarding the information and to treating people and their information with respect," notes Sarraille. And if those messages can be effectively conveyed when the complaint is being received, then the chances of them making an additional complaint to the HHS or seeking out a plaintiffs' lawyer to look at some tort theory, is dramatically reduced, he claims.

3. **Complaint in writing unnecessary.** While Sarraille says some people believe one should get the complainant to state his or her complaint in writing, he believes interactive dialogue is best, since it affords the provider the opportunity to get his message through. "It also gives the entity taking the complaint some ability to control obviously appropriately how these complaints are articulated on the document that they then produce." Sarraille says in some situations it may make sense to convey that information to counsel and to have it be an attorney-client privileged document.

4. **Forward the complaint to the appropriate sources.** The privacy officer normally interprets the complaints. Afterwards, he is then required to determine what the consequences of the complaint are, which may depend on the nature of the complaint as well as upon whom the focus of the complaint is made.

For example, says Sarraille, if the complaint is about a business associate and the claim is that the business associate has violated its agreement by failing to maintain privacy in some way, then that would trigger the legal obligation of the covered entity to mitigate the damages done by the violation. If it's not possible to mitigate those damages, then the covered entity must either terminate the business associate or report the associate to the DHHS.

5. **Follow up on complaints.** The information provided by a complainant must go immediately to whomever has the expertise to figure out what the HIPAA privacy consequences are of that particular complaint. After you've fixed the immediate problem, then the privacy officer should look more systematically. Subsequently, questions will need to be addressed, such as: What's wrong with our system that this has happened? Does this mean that we need to change our policies and procedures? Does it mean we need to send out a memo to all of our folks? Do we need to send memos on a quarterly basis to keep this issue in front of them? Is that enough to do it in writing? Do we have to really make this a focus of some training? Do we need to train everyone or just the front desk people on this?

   Those are the kinds of systematic questions that follow, says Sarraille. And if those questions are asked, the chances of repeated violations of HIPAA dwindles.