Final HIPAA Enforcement Rule Takes Effect

If you thought that the federal Health Insurance Portability and Accountability Act (HIPAA) lacked the “teeth” of enforcement, think again. The federal government has issued regulations that establish how the U.S. Department of Health and Human Services (HHS) will determine liability and calculate fines for health care professionals who violate any of the HIPAA Rules.

The HIPAA Enforcement Rule took effect in March 2006. The rule makes enforcement regulations applicable to all of the major HIPAA rules, including the Privacy and Security rules.

The HIPAA regulations pertain to covered entities including health care professionals whose activities “trigger” HIPAA. This happens, for example, when a psychologist transmits protected health information in submitting health care claims electronically. (See the article “What Triggers the Need to Comply?” on page 6 for additional information about actions that trigger HIPAA.)

This article highlights additional important aspects of the new Enforcement Rule that are important to psychologists: the general enforcement approach, liability for the acts of agents, fines and defenses available to a covered entity that is facing a penalty.

**General Enforcement Approach**

In deciding where to direct its enforcement efforts, HHS will rely primarily on complaints brought to the agency’s attention. However, HHS can conduct compliance reviews on its own if there has been no complaint. When acting on complaints, HHS is not limited to complaints by patients. For example, HHS can act on complaints from other covered entities.

Enforcement actions will remain private until a final penalty is imposed. So the fact that you may not have heard about HHS conducting investigations does not mean they are not taking place.

The Enforcement Rule generally favors a voluntary approach to HIPAA compliance whereby HHS would work with a psychologist at issue to make sure that the practitioner understands and corrects the violation. However, if such voluntary efforts fail, the rule calls for the agency to resort to investigations, hearings and fines.

**Liability for Actions of Your Agent**

The Enforcement Rule explains the circumstances under which you could be held liable for HIPAA violations of your agent—that is, someone acting on your behalf and at your direction. You can be subject to this type of “agency liability” if a member of your “workforce” commits HIPAA violations. The rule defines “workforce members” as including not only your paid employees, but also trainees and volunteers who are under your direct control.

You can also be held liable for violations by your agents who are not under your direct control but who are still carrying out HIPAA-related functions on your behalf. This kind of agent is generally considered a “business associate” under HIPAA, a person or company with whom you share protected health information as part of running your business. Examples include a billing service or accountant.

There is an important exception to HIPAA liability provided by the Enforcement Rule. You generally are not liable for the HIPAA violations of your business associate if you are in compliance with the business associate provisions of the Privacy and Security Rules as they apply to your practice. Essentially, this means that you have in place “business associate contracts” that comply with those rules. Importantly, however, this exception will not protect psychologists who are aware that their business associates are violating the privacy or security obligations under their contracts and fail to take reasonable steps to remedy the problem.

One place to find a business associate contract that satisfies both the Privacy Rule and Security Rule is in the HIPAA Security Rule Online Compliance Workbook available online at APAPractice.org.

**Fines**

The new Enforcement Rule allows HHS to impose fines of up to $100 per violation, to a maximum of $25,000 for violations of an identical requirement during one calendar year. A continuing violation is deemed a separate violation for each day it occurs. Thus, a continuing violation found to have lasted most of the year (at least 250 days) would reach the $25,000 limit for that one violation. In calculating the number of violations, HHS can rely on statistically valid sampling. However, the rule gives the accused entity a procedure for challenging those statistics.
HHS indicates that one act could give rise to several violations. The agency gives the example that the single act of disposing of a computer without first “scrubbing” the hard drive to remove electronic protected health information would violate several different HIPAA provisions.

In considering the amount of the fine, HHS will consider the nature and circumstances of the violation, the health professional’s history of prior compliance and his/her financial condition. More detailed considerations under the last category include the size of the covered entity and whether the fine would put the entity out of business.

When a proposed penalty becomes final, the enforcement process finally becomes public. HHS must notify the public of the fine imposed and the reason for imposing the penalty. HHS will also give notice to various other entities, including the appropriate state or local licensing agency and “the appropriate state or local medical or professional association.”

Available Defenses

The Rule provides several defenses that are available to someone facing a fine. If these defenses are established to HHS’ satisfaction, the agency will not impose a fine. The two most significant defenses for psychologists relate to not knowing about the violation and being unable to comply. The first of these defenses applies when covered entities who would be liable for penalty did not know that they were in violation, and by exercising reasonable diligence would not have known of the violation. The rule defines reasonable diligence as “the business care and prudence expected from a person seeking to satisfy a legal requirement” under similar circumstances. Obviously, practitioners could not reasonably rely on this defense if they failed to take steps to comply simply because they thought the federal government would not enforce the HIPAA rules.

The second defense applies when circumstances make it temporarily unreasonable for the entity to comply with the HIPAA requirement at issue, despite the exercise of ordinary business care and prudence. Under this defense, the entity knows they are violating a HIPAA rule and must normally correct the violation within 30 days of knowing about it.

For example, a devastating tornado destroys a psychologist’s practice, including paper and electronic copies of the privacy notice required by the HIPAA Privacy Rule. The psychologist sees new clients in the aftermath of the natural disaster but is unable to give them a copy of her privacy notice. She is able to correct the situation within 30 days by recreating the notice and distributing it to her new clients. If she were subject to an enforcement action, she could argue that she was temporarily unable to comply with this HIPAA requirement, despite the exercise of ordinary business care and prudence.

The entire text of the enforcement rule is available at http://www.hhs.gov/ocr/hipaa/FinalEnforcementRule06.pdf.

PLEASE NOTE: The information in this article does not constitute legal advice and should not be used as a substitute for obtaining personal legal advice and consultation prior to making decisions regarding your individual circumstances.