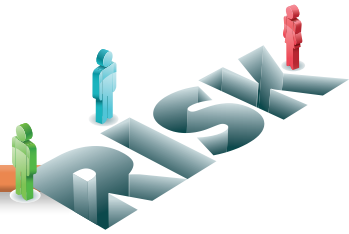

HIPAA violations and civil monetary penalties

Question: I recently experienced a possible breach of protected health information that stemmed from malware infecting my computer. I am a licensed professional counselor and have a solo private practice. I have reported the incident to my professional liability insurance carrier and am awaiting assignment of legal counsel to help me perform a risk assessment, figure out my obligations to report the breach, etc. However, I've been doing some research and became very concerned when I saw that something called "civil monetary penalties" can range up to $50,000 per violation, with a maximum annual limit of $1.5 million for certain HIPAA violations. Is this correct? What led to this possible breach was in no way intentional on my part. This type of penalty seems really unfair to counselors who don't have the same income as large health care entities do.

Answer: You are correct that the government can impose civil monetary penalties for certain categories of violations under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. However, there are two factors that sound like relatively good news for you.

First, HIPAA is "scalable," which essentially means that the government does not have the same expectations for a solo private practitioner that it does for a large hospital or health care entity. Second, this past spring, the U.S. Department of Health and Human Services issued notice that it was using its discretion to modify how it enforces the maximum annual limit of $1.5 million. This notice, published in the Federal Register on April 30, stated that the agency expects to engage in future rule-making to clarify the enforcement modifications (see *tinyurl.com/hipaaCMA*).

Without getting into the weeds, let's review a brief history of these laws and regulations and their enforcement. When HIPAA was enacted, Congress also established civil monetary penalties. These penalties were modified significantly after passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and its implementing regulations in 2013. The recent notice states that its intent is to resolve inconsistencies in the four penalty tiers. These tiers measured culpability depending on whether the violator exhibited:

1) No knowledge that HIPAA was being violated

2) Knowledge or reasonable cause to know that HIPAA was being violated if due diligence was applied

3) Willful neglect that was corrected

4) Willful neglect that was not corrected

Before the notice in April, the annual limit for all four tiers was set at $1.5 million. Following the notice, the annual limits were set as follows: $25,000 for the first tier, $100,000 for the second tier, $250,000 for the third tier and $1.5 million for the fourth tier.

You will want to work with your own attorney as soon as possible to perform a risk analysis. If you both find that a breach has occurred, you will want to take steps proactively to minimize harm and comply with reporting requirements. This action will be in the best interests of your clients and should help reduce any potential penalties that might be imposed on you.

~

For related resources, visit the American Counseling Association's professional development site at *aca.digitellinc.com/aca/* and search for the following titles:

- "Counselor Risk Management: What You Didn't Learn in Grad School That Could Lead to a Lawsuit or Licensure Board Complaint"
- "An APPLE a Day Keeps the Lawsuits at Bay"
- "Stay Ahead of the Curve: Learn to Minimize Professional Malpractice"
- "Counselor Risk Management: Counselors and Technology — A Two-Edged Sword"
- "Private Practice: The Ethics and HIPAA of Technology" ❖

Anne Marie "Nancy" Wheeler is an attorney licensed in Maryland and the District of Columbia. The information presented here is for educational purposes only. For specific legal advice, please consult your own local health care attorney.

Letters to the editor: *ct@counseling.org*