Phishing email targets HIPAA covered entities

Question: I'm a counselor in private practice, and I am a HIPAA (Health Insurance Portability and Accountability Act) covered entity. I received an email from the U.S. Department of Health and Human Services Office for Civil Rights that indicates I am being audited. Is this legitimate, and should I comply and respond by following the directions in the email?

Answer: The Health and Human Services Office for Civil Rights does have an audit program in place to review the policies and procedures adopted by HIPAA covered entities and their business associates (billing services, accountants, attorneys and other parties who are privy to protected health information). The aim is to ensure that covered entities and business associates are complying with the privacy and security rules under HIPAA and the "breach notification" requirements under HITECH (the Health Information Technology for Economic and Clinical Health Act). For basic information on HIPAA and HITECH compliance, see *hhs.gov/hipaa/for-professionals/index.html*.

Some email communications from the Office for Civil Rights regarding HIPAA/HITECH audits are legitimate. However, before automatically clicking any links in the email you received, be aware that the Office for Civil Rights issued an alert Nov. 28 regarding "phishing" emails that target HIPAA covered entities and their business associates. The phishing emails were disseminated on fake government letterhead under the signature of Jocelyn Samuels, the director of the Office for Civil Rights.

The alert warns that the phishing email "prompts recipients to click a link regarding possible inclusion in the HIPAA Privacy, Security, and Breach Rules Audit Program. The link directs individuals to a non-governmental website marketing a firm's cybersecurity services" (see *hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html*).

The bottom line is that you should compare the email address on the communication you received with the legitimate government email address, which is *OSOCRAudit@hhs.gov*. If you have received a legitimate request for information, you may wish to seek legal consultation regarding your response.

~

The question addressed in this column was developed from a deidentified composite of calls made to the Risk Management Helpline sponsored by the American Counseling Association. This information is presented solely for educational purposes. For specific legal advice, please consult your own local attorney. ❖

Anne Marie "Nancy" Wheeler, an attorney licensed in Maryland and Washington, D.C., is the risk management consultant for the ACA Ethics Department.

Letters to the editor:
ct@counseling.org