April 8, 2020

Beware of Fraudsters Posing as Government Investigators to Obtain Protected Health Information

Risk Management Question: What precautions can law firms, along with their lawyers and staff, take when they receive an unexpected request for protected health information (PHI) from someone claiming to be a representative of the Office of Civil Rights (OCR) or the Centers for Disease Control and Prevention (CDC)?

The Issue: The U.S. Department of Health and Human Services (HHS) and the Federal Bureau of Investigation (FBI) have warned about scammers posing as representatives from the OCR or CDC. The phony OCR Investigator may contact HIPAA-covered entities or their business associates to access PHI. The fake CDC representative may claim to have special information about COVID-19. These fraudsters prey on community fears and use threats of enforcement and fines to convince the unsuspecting individual to immediately provide the PHI of others.

Risk Management Solutions

Law firms and clients who maintain PHI should alert their employees about these scams and advise them to take the following actions:

- Always ask for the caller's name, title, phone number and email address.
- Ask for an OCR complaint transaction number or any other verifiable information relating to an OCR investigation.
- According to HHS, an OCR investigator's email address will end in @hhs.gov. If the caller provides a different domain name, it's a scam.
- Ask the caller to provide a confirmation email from a legitimate government email address.
- Verify the caller's identity and role by calling the main number listed on the website of the governmental entity they are purportedly from.
- Train employees to report suspected scams to a specific department within your firm and refrain from further communication with the caller until a supervisor has confirmed the request is legitimate.

Additional tips from the FBI:

- Do not open attachments or click links within emails from senders you don't recognize.
- Do not provide usernames, passwords, dates of birth, social security numbers, financial data, or other personal information—whether it be yours or someone else's—in response to an email or robocall.
- Always verify the web address of legitimate websites and manually type them into your browser.
- Check for misspellings or wrong domains within a link (e.g. an address that should end in ".gov" ends in ".com" instead).
- Suspected incidents of individuals posing as federal law enforcement should be reported to the FBI.

Always think before you click or answer the phone. Remember, let's be careful out there.

Steven M. Puiszis
312-704-3244
spuiszis@hinshawlaw.com

Noah D. Fiedler
414-225-4805
nfiedler@hinshawlaw.com

Joanna L. Storey
415-263-8143
jstorey@hinshawlaw.com

HINSHAW