

p.s.

Poyner Spruill^{LLP}
ATTORNEYS AT LAW

HHS Set to Identify by Name All Private Practices Experiencing a Breach Affecting 500 or More Individuals

05.26.2010

Elizabeth H. Johnson

As you know, HIPAA covered entities experiencing a security breach are obligated to notify affected individuals, the Department of Health and Human Services (HHS) and, in some cases, the media. When a breach affects 500 or more individuals, the covered entity must report the incident to HHS within 60 days of discovery. HHS, in turn, provides a brief summary of the event on its website, www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html.

To date, HHS has listed private practices anonymously, identifying them only as "Private Practice." HHS took the position that private practices could not be specifically named on the website because they are identifiable as "individuals" within the meaning of the Privacy Act which would potentially require the practice's consent prior to listing them by name. Pursuant to the Privacy Act, HHS may designate its publication of breaches, including naming private practices, as a "routine use" of the information such that prior consent is not required for the publication. Accordingly, on April 13, HHS published a Federal Register notice stating its intention to start identifying private practices by name on its breach website, designating such publication as a "routine use" of the information under the Privacy Act. HealthLeaders Media reports that HHS will begin naming private practices both prospectively and retroactively within 40 days of publishing the Federal Register notice, or May 23 at the earliest.

Private practices (and other HIPAA covered entities) should take steps to mitigate the risk of a security breach. Although a breach can occur in a variety of ways, almost half of the breaches reported on the HHS website were caused by lost or stolen electronic portable devices, such as laptops. In addition, BNA's Privacy Law Watch reports that 80% of medical identity theft cases are caused by health organizations' staff. As a result, portable media and dishonest employees are among the most likely causes of a security breach.

HIPAA covered entities also should implement a procedure to respond to suspected breaches, as mandated by recent revisions to the HIPAA Privacy Rule. A sound procedure will help covered entities, including private practices, to respond promptly to suspected breaches, enabling them to meet the 60-day reporting deadline if their investigation of the breach determines it must be notified to individuals and HHS.

p.s.

POYNER SPRUILL publishes this newsletter to provide general information about significant legal developments. Because the facts in each situation may vary, the legal precedents noted herein may not be applicable to individual circumstances. © Poyner Spruill LLP 2010. All Rights Reserved.

RALEIGH

CHARLOTTE

ROCKY MOUNT

SOUTHERN PINES

WWW.POYNERSPRUILL.COM

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075