Dinsmore&Shohl LLP
ATTORNEYS

Health Care Hot Topics (August 2009)

August 31, 2009

Stacey A. Borowicz , Larry L. Lanham II

New Federal Breach Notification Rules Are Finalized

Following the passage of the American Recovery and Reinvestment Act of 2009 (the "Recovery Act") last February, the Department of Health and Human Services ("HHS") and Federal Trade Commission ("FTC") have given marching orders to healthcare providers and related entities to provide breach notification in relation to compromised protected health information and other forms of individually identifiable health information ("HHS Rule" and "FTC Rule"). Any provider or business that handles health records should be aware of these new federal rules.

The HHS Rule: Breach Notification for Unsecured Protected Health Information

The new HHS Rule implements the Health Information Technology for Economic and Clinical Health ("HITECH") Act, which was included as part of the Recovery Act. HITECH mandates that Covered Entities and their business associates provide notification to affected patients when there is a "breach" of "unsecured" protected health information.[1] While there are nuances and exceptions that may apply, a "breach" generally occurs anytime there is an "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information."[2] What constitutes "unsecured" protected health information is a more technical question. Essentially, it means "protected health information that is not secured through the use of a technology or methodology" that renders protected health information "unusable, unreadable, or indecipherable to unauthorized individuals."[3] Depending on the nature of the breach, the HHS Rule may require notice to affected patients, the Secretary of HHS, and the media.[4] The HHS Rule also outlines the specific content within notifications, such as a description of what happened, the type of information involved, steps individuals should take to protect themselves from harm, and contact information to learn more information.[5]

The FTC Rule: Breach Notification for Vendors of Unsecured Personal Health Records With Individually Identifiable Health Information

The new FTC Rule was created in parallel to the HHS Rule. The idea is to impart similar notification requirements in the context of new web-based entities that collect health information. As a consequence, the FTC rule applies to "vendors of personal health records ["PHR"], PHR related entities, and third party service providers."[6] If "unsecured" and "PHR individually identifiable health information" is breached, the FTC Rule requires notification of the respective customer (*e.g.*, the individual, hospital, physician group, etc.), and possibly the FTC and media.[7] A "breach" generally occurs anytime there is an unauthorized acquisition of a personal health record that personally identifies the individual.[8] In order to avoid any redundancy, the definition of what constitutes "unsecured" information for the FTC Rule is the same as the HHS Rule.[9]

Providers and other entities that handle individual health records and information are well-advised to consult legal counsel in the event of a known or suspected breach. For more details, the HHS Rule may be found here, and the FTC Rule may be found here.

---

[1] Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42740 (Aug. 24, 2009), codified at 45 C.F.R. Parts 160 and 164. Covered Entities and business associates relates to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").
[2] *Id.* at 42741.
[3] *Id.*
[4] 45 C.F.R. § 164.404–410.
[5] *Id.* at § 164.404(c).
[6] 16 C.F.R. § 318.1.
[7] *Id.* at § 318.3.
[8] *Id.* at § 318.2.
[9] *Id.* at § 318.2(i).