ALERT
OCTOBER 1, 2008

HEALTH LAW
News Concerning
Recent Health Law Issues

COZEN O'CONNOR
www.cozen.com

HHS' FIRST RESOLUTION AGREEMENT FOR ALLEGED HIPAA VIOLATIONS AND WHAT IT MEANS FOR YOU

Melanie K. Martin, Esq. • 215.665.2724 • *mmartin@cozen.com*

The Department of Health and Human Services ("HHS") has entered into its first resolution agreement with a covered entity to settle alleged violations of the Health Insurance Portability and Accountability Act's ("HIPAA") privacy and security rules.[1] According to HHS, the resolution agreement with Providence Health & Services ("Providence"), a Seattle-based not-for-profit health system, addresses a series of "covered incidents" involving the loss of individually identifiable health information.

Specifically, HHS alleges that on several occasions in 2005 and 2006, backup tapes, optical disks, and laptops, all containing unencrypted electronic protected health information, were removed from the Providence premises by employees and left unattended. The media and laptops were subsequently stolen, compromising the protected health information of over 386,000 patients. HHS received over 30 complaints about the stolen information after Providence informed patients of the theft pursuant to state notification laws. Providence also reported the stolen media to HHS.

THE RESOLUTION AGREEMENT

Pursuant to the resolution agreement, Providence agreed to pay a $100,000 "resolution amount" and implement a detailed corrective action plan. The corrective action plan requires Providence to revise its policies and procedures regarding physical and technical safeguards, train workforce members on the safeguards, conduct audits and site visits of facilities, and submit compliance reports to HHS. Providence is subject to the agreement for three years, during which time HHS may impose civil monetary penalties for Providence's failure to comply with any requirements.

STEPPED UP ENFORCEMENT

Although this resolution agreement is the first, it is likely not the last. In an HHS press release, Winston Wilkinson, director of the Office of Civil Rights ("OCR"), affirmed OCR's commitment to "effective enforcement of health information privacy and security protections" and warned that other covered entities not in compliance with the privacy and security rules "may face similar action." Consistent with this warning, the CMS Office of E-Health Standards and Services and its contractor, PricewaterhouseCoopers, undertook the first of between 10 and 20 on-site HIPAA security compliance reviews they expect to perform by December 2008. In addition, it is widely believed that the Office of Inspector General has conducted HIPAA security compliance audits similar to the well-publicized audit at Piedmont Hospital in March 2007, though the details and results of these audits have not been disclosed.

WHAT CAN YOU DO?

For covered entities that wish to prevent security breaches and maintain effective compliance, the terms of the corrective action plan may constitute privacy and security "best practices." As such, covered entities may wish to:

- review privacy and security policies and procedures, as well as administrative, physical and technical safeguards to ensure they address current uses and sources of healthcare data and evolving information security threats;[2]
- evaluate privacy and security risks, document risks, the decision-making process and proposed changes, and implement changes;
- continuously monitor security and privacy practices to ensure they are enforced; and

1. The resolution agreement is available at: http://www.hhs.gov/ocr/privacy/enforcement/agreement.pdf.

2. For strategies to protect electronic protected health information stored on portable media/devices, *see* HHS' December 2006 "HIPAA Security Guidance," available at: http://www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806.pdf.

- engage in periodic HIPAA training of employees and other individuals who have access to individually identifiable health information.

A covered entity should also develop and implement policies and procedures specific to portable devices, such as laptops and PDAs, to ensure that employees who use such devices are knowledgeable of security risks and applicable policies and procedures. In addition, a covered entity may wish to routinely inventory all portable devices and media to better allow for timely detection of, and response to, security breaches.

While such steps will not serve as a guarantee against security breaches, they will set the stage for effective compliance and minimize the potential for penalties in the event of a HIPAA audit.

For more information on HIPAA privacy and security compliance, or to learn additional ways in which you can protect patient or client information, please contact John Washlick at 215.665.2134 (jwashlick@cozen.com), Kate Layman at 215.665.2746 (klayman@cozen.com), or Melanie Martin at 215.665.2724 (mmartin@cozen.com).

COZEN O'CONNOR HEALTH LAW PRACTICE GROUP

Mark H. Gallant, Co-Chair ..... 215.665.4136 ..... mgallant@cozen.com
John R. Washlick, Co-Chair ..... 215.665.2134 ..... jwashlick@cozen.com
Gregory Fliszar ..... 215.665.7276 ..... gfliszar@cozen.com
Kimberly Bane Hynes ..... 215.665.2022 ..... khynes@cozen.com
Katherine M. Layman ..... 215.665.2746 ..... klayman@cozen.com
Melanie Martin ..... 215.665.2724 ..... mmartin@cozen.com
E. Gerald Riesenbach ..... 215.665.4159 ..... eriesenbach@cozen.com
Salvatore G. Rotella, Jr. ..... 215.665.3729 ..... srotella@cozen.com
Judy Wang ..... 215.665.4737 ..... jwang@cozen.com