DechertOnPoint

July 2007 / Special Alert

A legal update from Dechert's Employee Benefits and Executive Compensation and Health Law Groups

HIPAA Security Alert: HIPAA Audit and Other News

Several years have passed since the April 2005 compliance date for the HIPAA Security Rule. Although many health plans and health care providers conducted security risk analyses and implemented security safeguards and policies and procedures, some have not completed this process. However, recent activities of the Office of Inspector General ("OIG") and the Department of Health and Human Services ("DHHS") would suggest that health plans and health care providers should seriously consider finishing and/or re-evaluating their risk assessments and risk managements policies and procedures, especially those relating to remote use of electronic protected health information.

OIG Audit

Perhaps spurred by public reports of security breaches involving electronic health information and by criticism that the DHHS has not rigorously enforced HIPAA, the OIG has begun conducting an audit of a covered entity related to HIPAA security. Specifically, it has been announced that Piedmont Healthcare, Inc. in Atlanta is being audited by the OIG. However, because this audit is being conducted by the OIG and not the Centers for Medicare and Medicaid Services ("CMS"), the DHHS division to which authority for HIPAA Security Rule enforcement has been delegated, it is not clear whether this is a true HIPAA security audit.

In the OIG Work Plan for Fiscal Year 2007, the OIG notes that it plans to review CMS's experience implementing the HIPAA privacy and security regulations for the Medicare and Medicaid Programs in an effort to identify key issues for the DHHS's health information technology initiative. According to the Work Plan, the primary objective of this initiative is to foster the use of electronic medical records throughout the health industry, which the OIG believes will further economic and efficient delivery of health services and enhance patient safety.

The OIG noted, however, that the "wider use of electronic medical records and personal health records raises concerns over privacy and security of patient data." It is possible that the audit mentioned above is part of the OIG's efforts to broaden the scope of its review beyond CMS's HIPAA implementation experience.

CMS HIPAA Security Guidance

In December 2006, CMS issued guidance regarding remote access to electronic protected health information ("EPHI") through portable devices or on external systems or hardware not owned or managed by a covered entity. This guidance lists strategies for covered entities that conduct some of their business activities though:

- the use of portable media/devices (such as USB flash drives) that store EPHI, and
- offsite access or transport of EPHI via laptops, personal digital assistants (PDAs), home computers or other non corporate equipment.

CMS also lists other devices and tools that raise concerns because of their vulnerability: smart phones, hotel, library and other public workstations, wireless access points, memory cards,

floppy disks, CDs, DVDs, backup media, e-mail, and remote access devices. CMS notes that covered entities should be extremely cautious about allowing the offsite use of, or access to, EPHI. CMS nonetheless realizes that there are some appropriate offsite uses of EPHI, including a home health nurse collecting and accessing patient data using a PDA or laptop during a home health visit.

For such offsite uses of EPHI, CMS recommends that covered entities place significant emphasis and attention on their risk analysis and risk management strategies, policies and procedures for safeguarding EPHI, and security awareness and training regarding such policies and procedures. With regard to risk analysis and risk management, CMS noted that, among other things, data access policies and procedures should focus on ensuring that users only access data for which they are appropriately authorized based on their role within the organization and their need to access such data.

Storage policies and procedures must address security requirements for media and devices which contain EPHI and are moved beyond the covered entity's physical control. Transmission policies also must focus on ensuring the integrity and safety of EPHI sent over networks, and address both direct exchange of data and remote access to applicants hosted by the organization (such as a provider's home access to ePrescribing systems). At a minimum, CMS recommends that training programs should provide clear and concise instructions for accessing, storing and transmitting EPHI, including EPHI accessed remotely.

CMS also notes that the entity's security incident procedures must specify the actions workforce members must take to manage harmful effects of a loss, should a covered entity experience loss of EPHI via portable media. The guidance contains a table which lists risks applicable to each category (access, storage, transmission), and pairs each category with possible risk management strategies. Covered entities should evaluate whether these possible risk management strategies would be appropriate for their organizations.

Potential HIPAA Security Rule Regarding Remote Security Standards

On April 30, 2007, DHHS published its Semiannual Regulatory Agenda. This agenda includes notice of a rule to be proposed that would "further address the existing compliance requirements of the HIPAA Security regulations specific to covered entities that allow offsite access to, or use of, electronic protected health information."

DHHS notes that the proposed rule is necessary because of "several recent security incidents related to the use of laptops, other portable and mobile devices and external hardware that store, contain, or are used to access electronic protected health information." The purpose of the proposed rule is to provide a more "prescriptive set of remote security requirements designed to reduce the likelihood of unauthorized uses and disclosures of sensitive health information."

The very tentative date for publication of this proposed rule is July 2007. Actual proposed rule publications, however, rarely follow these estimated timetables.

■ ■ ■

Health plans (including employer group health plans) and health care providers should consider reevaluating their HIPAA compliance program in light of recent CMS guidance. In order to be better prepared for a future proposed rule relating to remote access to EPHI, covered entities should compare their risk management strategies relating to remote access, storage, and transmission of EPHI to the "possible risk management strategies" listed by CMS in its December 2006 guidance.

Practice group contacts

If you have questions regarding the information in this legal update, please contact the Dechert attorney with whom you regularly work, or any of the attorneys listed. Visit us at www.dechert.com/employeebenefits or www.dechert.com/health.

Robert W. Ballenger
Philadelphia
+1 215 994 2208
robert.ballenger@dechert.com

Susan M. Hendrickson
Princeton
+1 609 620 3206
susan.hendrickson@dechert.com

David F. Jones
Chair, Employee Benefits and Executive Compensation
Philadelphia
+1 215 994 2822
david.jones@dechert.com

Jan P. Levine
Chair, Health Law
Philadelphia
+1 215 655 2440
jan.levine@dechert.com

Beth L. Rubin
Philadelphia
+1 215 994 2535
beth.rubin@dechert.com

Teresa L. Salamon
Philadelphia
+1 215 994 2273
teresa.salamon@dechert.com

David N. Sontag
Philadelphia
+1 215 994 2576
david.sontag@dechert.com

Dechert LLP

www.dechert.com

U.S.

Austin
Boston
Charlotte
Hartford
New York
Newport Beach
Philadelphia
Princeton
San Francisco
Silicon Valley
Washington, D.C.

UK/Europe

Brussels
London
Luxembourg
Munich
Paris