APRIL 2007

IN THIS ISSUE

Connecticut Court Holds that Strict Compliance with HIPAA May Not Be Possible or Necessary in Discovery

BACKGROUND

Since the time of their passage, the privacy regulations promulgated under the Health Insurance Portability & Accountability Act ("HIPAA") have allowed covered entities to disclose protected health information ("PHI") in the course of a lawsuit. The regulations allow a covered entity to produce PHI during litigation either in response to: (i) a court order; or (ii) a subpoena, discovery request, or other lawful process served by a party to the proceeding. If the PHI is requested by means other than a court order, the requesting party must also provide satisfactory assurance to the covered entity that the PHI will be protected. For example, the party could file a qualified protective order ("QPO") with the court providing that the PHI will only be used for purposes of the litigation and either will be destroyed or returned to the covered entity at the conclusion of the case.

These regulations strike a balance between the sometimes competing right to medical privacy and right to open courts. By limiting the disclosure of PHI to the circumstances described above, the drafters of the privacy regulations sought to ensure that courts and litigants would take extra steps to safeguard the confidentiality of medical information disclosed in a lawsuit. This goal was accomplished in part by requiring parties and covered entities to observe formal regulatory procedures before producing medical information in the context of litigation.

A recent ruling in a Connecticut District Court, however, suggests that a QPO is sufficient to permit a covered entity to disclose PHI in connection with ex parte interviews resulting from litigation where no

subpoena or compulsory process has been issued.

THE LAWSUIT

The plaintiff was an adult resident of a group home regulated by the Connecticut Department of Mental Retardation ("DMR"). The plaintiff alleged that the group home provided her with substandard care that resulted in physical harm. In or about May 2004, the plaintiff filed a lawsuit in federal district court in Connecticut naming the DMR, the group home, and other health care professionals as defendants. Among other relief, the plaintiff sought an order to compel DMR to engage in a system-wide reform of its policies regarding the operation of adult group homes.

THE INFORMAL INVESTIGATION

DMR retained three experts in defense of the case. The defense experts sought to conduct an informal investigation of the facts by interviewing employees of the group home outside of the presence of plaintiff's counsel. DMR did not issue a subpoena or any formal discovery request compelling the group home to cooperate in the investigation. Instead, the investigation was to be conducted informally and with the consent and cooperation of the group home operator. The plaintiff objected to these interviews on the ground that her rights under HIPAA would be violated to the extent that the group home employees discussed her medical information with the defense experts.

THE RULING

On January 25, 2007, the Connecticut district court held that HIPAA did not prohibit the informal interviews from going forward. Despite the fact that the interviews were not compelled by a formal discovery request, as previously believed to be required under HIPAA, the court held that HIPAA permits the disclosure of medical information during an informal interview provided that a QPO is in place. Because a QPO had already been entered in the case, the court permitted the informal interviews to be conducted. However, the court ordered the parties to reexamine whether plaintiff's counsel should be present during the interviews.

CONCLUSION

The ruling in this case demonstrates that courts may permit discovery without compulsory process when dealing with medical privacy issues so long as certain protections are in place. Strict compliance with the regulatory language of HIPAA would have required that the group home employees participate in the interviews only if subject to compulsory process. Nonetheless, the court allowed the informal interviews to take place without requiring the DMR to take the formal step of issuing a subpoena or deposition notice to the covered entity.

The Robinson & Cole Health Law Group has experience advising covered entities regarding their obligations to secure and safeguard confidential information under HIPAA. For assistance, please contact any member of the Health Law Group.

Have You Taken Adequate Steps to Safeguard ePHI?

The Department of Health and Human Services ("HHS") recently issued guidance under the Health Insurance Portability and Accountability Act ("HIPAA") security rule ("Security Guidance") setting forth risk management strategies for organizations that use or permit access to electronic protected health information ("ePHI") outside of the organization's physical environment. Such use or disclosure may involve accessing, storing, or transmitting ePHI through vulnerable devices such as USB flash drives, laptops, personal digital assistants, home computers, or other remote access devices. Pursuant to the HIPAA Security Rule, all covered entities are required to regularly ensure the confidentiality, integrity and availability of all ePHI that the covered entity creates, receives, maintains, or transmits. As such,

covered entities must analyze the potential risks and vulnerabilities associated with the access, storage and transmission of ePHI from offsite locations and develop risk management measures to reduce such risks and vulnerabilities. A summary of potential risks and respective strategies outlined by HHS is provided below.

ACCESSING ePHI

The risks involved in providing users access to ePHI from offsite locations include, but are not limited to, log-on or password information being lost or stolen, unauthorized users gaining access through unattended offsite workstations and systems getting contaminated by a virus introduced from an infected external device. The risk of losing or someone stealing log-on or password information could be diminished by: (i) implementing a two-factor authentication for granting remote access to systems that contain ePHI, (ii) requiring factors beyond general usernames and passwords to gain access to systems; (iii) implementing a technical process for creating unique user names; and (iv) performing authentication when granting remote access to a workforce member.

The risk of unauthorized users accessing ePHI through unattended offsite workstations could be diminished by establishing appropriate procedures for session termination on inactive portable or remote devices. Systems being contaminated by a virus introduced from an infected external device could be diminished by: (i) installing personal firewall software on all laptops that store or access ePHI or connect to networks on which ePHI is accessible; and (ii) installing, using and regularly updating virus-protection software on all portable or remote devices that access ePHI.

STORING ePHI

The risks involved in storing ePHI on remote or portable devices include, but are not limited to, the unauthorized access to or modification of ePHI stored on a lost or stolen portable device, the loss of operationally critical ePHI on a remote device, the loss or theft of ePHI left on devices after inappropriate disposal by the organization, leaving data on an external device and systems being contaminated by a virus introduced from a portable storage device. The unauthorized access to or modification of ePHI stored on a lost or stolen portable device could be diminished by: (i) identifying the types of hardware and electronic media that must be tracked and developing inventory control systems; (ii) maintaining a record of person(s) responsible for or permitted to use hardware and electronic media containing ePHI; (iii) requiring use of lock-down or other locking mechanisms for unattended laptops; (iv) password protecting files and all portable or remote devices that store ePHI; (v) requiring that all portable or remote devices that store ePHI employ encryption technologies of the appropriate strength; and (vi) developing processes that ensure appropriate security updates are deployed to all portable devices.

The loss of operationally critical ePHI on a remote device could be diminished by: (i) ensuring that a backup of all ePHI entered into remote systems is created; and (ii) developing a policy to encrypt backup and archival media. The loss or theft of ePHI left on devices after inappropriate disposal by the organization may be diminished by establishing ePHI deletion policies and media disposal procedures.

Leaving data on an external device may be diminished by: (i) prohibiting or preventing the download of ePHI onto remote systems or devices without an operational justification; (ii) ensuring the workforce is appropriately trained on policies that require users to search for and delete any files intentionally or unintentionally saved to an external device; and (iii) minimizing the use of browser-cached data (temporary storage in memory or on disk that holds the most recently viewed Web pages) which manage ePHI. Systems being contaminated by a virus introduced from a portable storage device may be diminished by installing virus-protection software on all portable or remote devices that store ePHI.

TRANSMITTING ePHI

The risks involved in transmitting ePHI over an electronic communications network include, but are not

limited to, the interception or modification of data during transmission and systems being contaminated by a virus introduced from an external device used to transmit ePHI. The interception or modification of data during transmission may be diminished by: (i) prohibiting the transmission of ePHI via open networks, such as the Internet, where appropriate; (ii) prohibiting the use of offsite devices or wireless access points, i.e. hotel workstations, for non-secure access to email; and (iii) mandating appropriately strong encryption solutions for the transmission of ePHI. Systems being contaminated by a virus introduced from an external device used to transmit ePHI may be diminished by installing virus-protection software on portable devices that can be used to transmit ePHI.

In light of the high number of security incidents related to the use of portable devices and external hardware that are used to access, store, or transmit ePHI, health care facilities and providers must consider reviewing and revising their policies and procedures to protect ePHI. If you need assistance interpreting the Security Guidance or reviewing and revising policies and procedures in accordance with HIPAA and the Security Guidance, please contact a member of Robinson & Cole's Health Law Group.

It is Time to Audit Your Compliance with the HIPAA Privacy Rule

The Privacy Rule promulgated pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") requires that health care providers, health plans and health care clearinghouses covered by HIPAA ("Covered Entities") implement policies and procedures to reasonably safeguard protected health information ("PHI") from any intentional or unintentional use or disclosure in violation of HIPAA. Almost four years after the implementation of the Privacy Rule, reports from the United States Department of Health and Human Services Office of Civil Rights ("OCR"), which is charged with enforcing the Privacy Rule, indicate that complaints involving violations of the Privacy Rule are being filed at an increasing rate. It appears that OCR is becoming more diligent in investigating Covered Entities' compliance with the Privacy Rule and is likely to become less tolerant of omissions and mistakes. In order to avoid potential HIPAA violations that could result in penalties and liability, Covered Entities should audit their compliance with the Privacy Rule. Non-compliance can result in civil money penalties ($100 per violation up to $25,000 per entity per year per violation) or criminal liability for "wrongful disclosures" (up to $250,000 and up to 10 years in prison).

Auditing compliance with the Privacy Rule may assist Covered Entities in correcting deficiencies before a violation occurs and may reduce the potential liability associated with wrongful use and disclosure and costs involved in responding to an OCR-initiated investigation. Some mechanisms for assessing a Covered Entity's compliance include, without limitation, (i) reviewing the Covered Entity's HIPAA compliance policies and procedures to determine if they are current and complete; (ii) interviewing employees, including management to determine whether actual practices of the Covered Entity comply with HIPAA and the Covered Entity's policies and procedures; (iii) testing the Covered Entity's systems, such as sending noncompliant requests for access to PHI and using a test "patient" to determine if the Notice of Privacy Practices is given to the test "patient;" and (iv) conducting physical site audits to determine if the actual practices of the Covered Entity comply with HIPAA and the Covered Entity's policies and procedures. Following the audit, the Covered Entity must implement an internal corrective action plan that may include revising policies and procedures, implementing operational changes and training workforce members based on areas of actual or potential noncompliance.

Covered Entities should assess their compliance with the Privacy Rule. If you have any questions regarding the Privacy Rule or need assistance in auditing your compliance with the Privacy Rule, please contact any member of Robinson & Cole's Health Law Group.

Robinson & Cole's Health Law Group includes:

Lisa Boyle (co-chair) *Theodore J. Tucci (co-chair)*

Bradford S. Babbitt *Karen P. Conway*

Michael J. Kolosky *David M. Mack*

Brian D. Nichols *Tracey E. Scraba*

For more information, please contact Lisa Boyle at lboyle@rc.com
or 800-826-3579.