

March 23, 2007

Hall, Render, Killian, Heath & Lyman is a full service health law firm with offices in Indiana, Kentucky, Michigan and Wisconsin. Since the firm was founded by William S. Hall in 1967, Hall Render has focused its practice primarily in the area of health law and is now recognized as one of the nation's preeminent health law firms serving clients in multiple states. For more information visit us at www.HallRender.com.

Office Locations

Indiana Offices

Downtown

One American Square
Suite 2000

Indianapolis, IN 46282
(317) 633-4884

Contact: Mark Swearingen

North Office

8402 Harcourt Road
Suite 820

Indianapolis, IN 46260
(317) 871-6222

Contact: Jim Willey

Kentucky Office

614 West Main Street
Suite 4000

Louisville, KY 40202
(502) 568-1890

Contact: Rene Savarise

Michigan Office

Columbia Center, Suite 315
201 West Big Beaver Road
Troy, MI 48084

(248) 740-7505

Contact: Michael Philbrick

Wisconsin Office

411 E. Wisconsin Avenue
Suite 900

Milwaukee, WI 53202
(414) 721-0442

Contact: Monica Hocum

Contact Us

hallrender@hallrender.com

OIG Initiates HIPAA Security Audit

How would your organization fare if the Department of Health and Human Services Office of the Inspector General ("OIG") decided to audit the organization's compliance with the HIPAA Security Rule? That is precisely the situation faced by a Georgia hospital. As we approach the first anniversary of the effective date of the HIPAA Enforcement Rule, as providers struggle with the uncertainties of implementing electronic medical records, and amid countless stories of breaches resulting from unscrupulous individuals and stolen laptops, the OIG has initiated an audit of a health care provider's compliance with the Security Regulations. The OIG's Office of Audit Services performs all auditing services for the Department of Health and Human Services ("HHS"). The audits are designed to examine the performance of HHS programs and those who implement or participate in those programs.

While the OIG has performed security audits of many State Medicaid Systems, this is the first security audit of a private entity that has come to our attention. Although there has been no official word, it is thought that this audit is being conducted on a "pilot" basis. Therefore, covered entities should anticipate increased Security Rule audit activity in the future.

The audit letter, which came with relatively little advance notice of the OIG's initial on-site visit, was accompanied by an extensive information request. The contents of the request can be grouped into several categories and included requests for policies and procedures as well as other information related to the hospital's storage, processing and transmission of electronic protected health information ("ePHI"). The following is a summary of the information requested.

Safeguards

- Information about anti-virus systems, firewalls, routers and switches.
- Identification of physical safeguards for electronic information systems, including maintenance and repairs of hardware, walls, doors and locks in sensitive areas.
- What measures the entity has taken to prevent, detect, contain and correct violations.
- Delineation of authorized methods for transmission of ePHI.
- Details about passwords and server configuration.
- Information pertaining to computer patch management.
- Identification of and provide access to contracts related to outsourced individuals and contractors with access to ePHI.
- Specifics about the entity-wide security program plans.
- Identification of system administrators, backup operators, and users.
- Lists of database security requirements and settings.
- Lists of all primary domain controllers and servers and whether the servers are used for processing, maintaining, updating, and/or storing ePHI.

Access

- How users' access to ePHI is established and terminated.
- Identification of security access controls.

- Mechanisms used to obtain emergency access to electronic information systems.
- Technical information related to remote access (e.g., network infrastructure, access servers, authentication and encryption software).
- Transmission and usage of wireless access.
- Identification of all users with access to ePHI data, including each individual's access rights and privileges.
- Identification of software used to manage and control access to the internet.

Assessment, Monitoring and Sanctions

- Disclosure of risk assessments and analysis of systems that house or process ePHI.
- Use and processing of audit logs, access reports, and incident reports.
- Examples of how security violations are logged and monitored.
- Response to employee violations related to ePHI.

As you review the information requested in the audit, keep in mind that the Security Rule were designed to be flexible and scalable. We recommend that your organization document the rationale for its decisions regarding implementation of the security standards and, if applicable, the decision not to formally implement measures related to the addressable standards. Although we do not have specific information about the OIG's plans for other audits, all covered entities should proceed as though there will be others.



About the Authors

Mark Swearingen is an attorney in the Indianapolis office of Hall Render. He concentrates his practice in health law and coordinates the firm's HIPAA practice. He is admitted to practice in Indiana, Illinois and Missouri. Mark can be contacted at (317) 977-1458 or by e-mail at mswearingen@hallrender.com.

Monica Hocum is an attorney in the Milwaukee office of Hall Render. She concentrates her practice in health law, including HIPAA security issues. She is admitted to practice in Wisconsin. Monica can be contacted at (414) 721-0454 or by e-mail at mhocum@hallrender.com.

This publication is intended for general information purposes only and does not and is not intended to constitute legal advice. The reader must consult with legal counsel to determine how laws or decisions discussed herein apply to the reader's specific circumstances.