THE OCR AUDITORS ARE COMING - ARE YOU NEXT?

WHAT TO EXPECT AND HOW TO PREPARE

ROPES
&GRAY

On June 10, 2011, the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") awarded KPMG a $9.2 million contract to develop a pilot HIPAA audit program mandated under the HITECH Act of 2009 to ensure compliance with the HIPAA Privacy and Security Rules and Breach Notification standards.

Between November 2011 and December 2012, the OCR will audit up to **150** covered entities.

WHAT IS MY RISK?

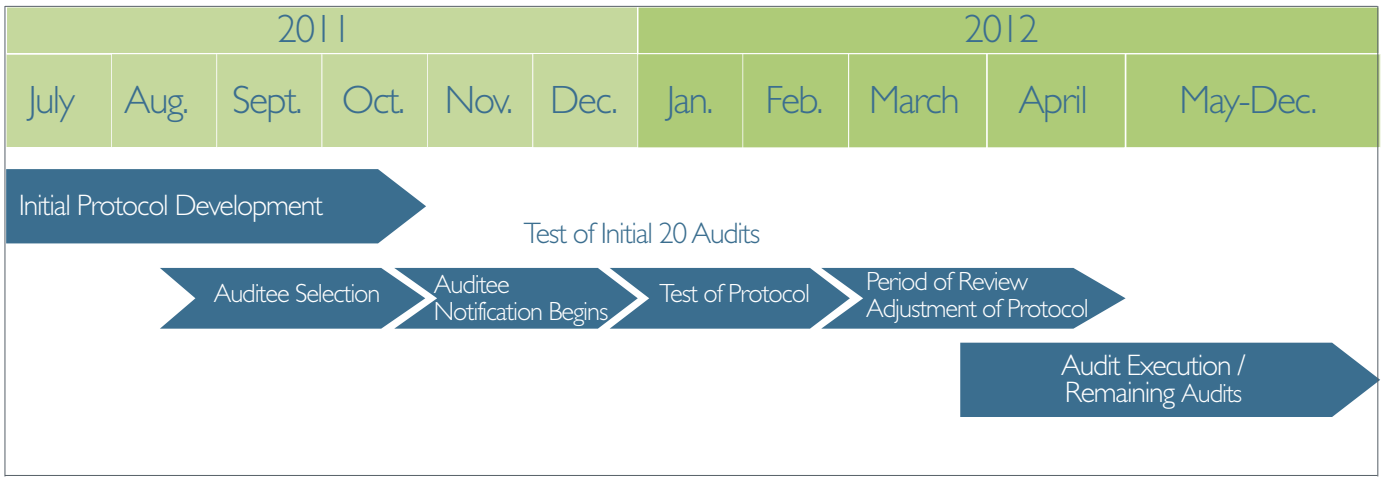
OCR has made clear that enforcement actions may follow audits revealing significant HIPAA Security compliance issues. In recent years, OCR has stepped up its enforcement activity:

- **Massachusetts General Hospital.** $1 million settlement and three-year Corrective Action Plan for loss of Protected Health Information ("PHI") by employee. (February, 2011)
- **Cignet Health**. $4.3 million penalty for refusing patients access to their medical records. (February, 2011)
- **UCLA Health System**. $865,000 settlement and three-year Corrective Action Plan for allowing unauthorized access to patient medical records. (July, 2011)

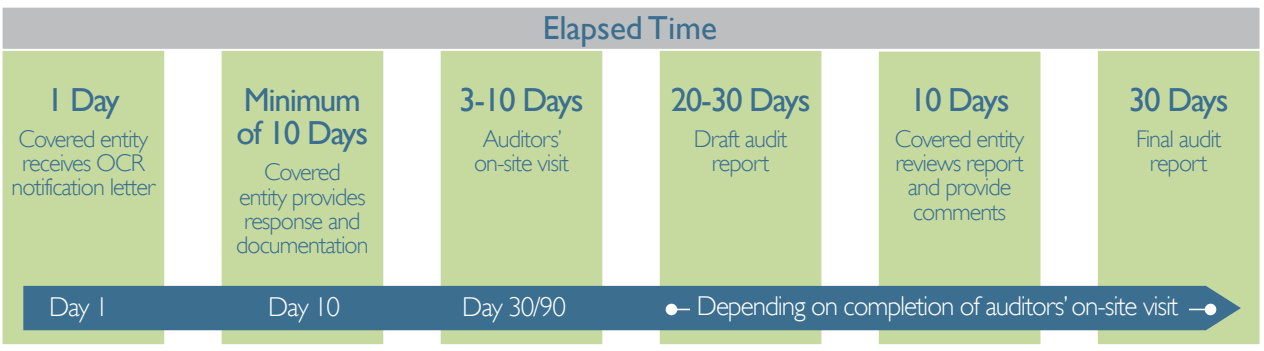
WILL MY ORGANIZATION BE NEXT?

The initial HIPAA audit program is focused on HIPAA-covered entities (i.e. health care providers, health plans and health care clearinghouses). With 150 audits planned and an aggressive timeline, covered entities should not be surprised to receive an audit request.

WHEN WILL THE AUDITS BEGIN?



HOW LONG DOES THE AUDIT TAKE?



WHAT WILL THE ON-SITE VISIT LOOK LIKE?

- Interviews with key organizational leaders;
- Scrutiny of physical operations controls (i.e. storage, maintenance and use of PHI);
- Assessment of how well organizational policies and procedures meant to protect PHI are implemented in practice by the organization;
- Identification of areas of concern with respect to general regulatory compliance.

WHAT WILL THE AUDITORS FOCUS ON?

OCR has not yet released a set of audit questions. In May 2011, however, the HHS Office of Inspector General ("HHS-OIG") issued a report based on the agency's audits of seven hospitals across the country. The report identified a number of vulnerabilities, which are likely to be high on OCR's list of priorities. Areas of vulnerability included:

- Inadequate security of wireless networks
- Lack of adequate updates to software and operating systems
- Access log recordkeeping
- Insufficient incident detection and response procedures
- Inadequate user access controls and password management controls
- Risk of theft or loss of mobile devices
- Information access management, including role-based access

"High impact" vulnerabilities are vulnerabilities that may (1) result in the highly costly loss of major tangible assets or resources; (2) significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) result in human death or serious injury.

The "HHS-OIG" report also placed particular emphasis on so-called "high impact" vulnerabilities. The vast majority of high impact vulnerabilities related to lacking or insufficient technical safeguards (i.e. insufficient wireless access control, audit control, integrity control, and person or entity authentication and transmission security). We expect that OCR auditors will focus attention on these high impact vulnerabilities.

HOW SHOULD MY ORGANIZATION PREPARE?

The HHS-OIG report provides a good starting point for identifying vulnerabilities that may be the focus of the OCR audits. Developing a work plan and reviewing your operations in light of the vulnerabilities identified in the report may help reduce the risks of adverse findings in an audit. To help you in this effort, our Health Care Privacy and Data Security attorneys have developed the attached checklist.

Your preparation should also include:

- A review of your policies and procedures to ensure compliance with the HIPAA Security Rule;
- A review and update as necessary of your organization's risk assessment plan;
- Updates to your privacy and security safeguards and implementation of corrective actions when necessary;
- Updating of your training and workforce education materials as necessary.

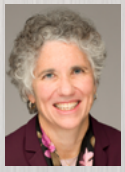
HOW WE CAN HELP

We know more than just the law – we know the health care industry, health care operations, and health care information systems. Our advice and solutions to privacy, security, and data breach issues address practical, operational and business concerns. We do not provide advice in a vacuum; we seek to solve data privacy and security matters in a way that meets our clients' business needs.

We can help your organization identify and assess organizational risk related to the HIPAA Security Rule and OCR audit program. We have assisted covered entities in responding to HIPAA security rule audits and enforcement actions, and we have developed corrective action programs.

More generally, our attorneys have extensive experience advising a broad range of health care clients in connection with data privacy and security matters, including compliance with the HIPAA Privacy and Security Rules and the HITECH Act. We advise both covered entities and business associates with respect to the permitted uses and disclosure of protected patient information, billing and payment issues, transaction related issues and the development of policies and procedures for HIPAA and HITECH privacy and security compliance. We also assist clients with the conduct of risk assessments and gap analyses, training of workforces, remediation of known HIPAA compliance matters, and prevention of data disclosure breaches. We have worked closely with clients in connection with responding to state and federal regulatory authorities in the wake of data breaches, including compliance with state and federal reporting and notification obligations, responding to audits and investigations by regulatory authorities, implementation of remedial changes to privacy and security compliance, and employee training and employee discipline related to data privacy and security matters.

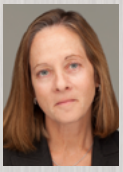
If you have questions about these issues or other topics related to health care privacy and data security, please contact your Ropes & Gray attorney or a member of the Health Care Privacy and Data Security team listed below:



Michele M. Garvin

michele.garvin@ropesgray.com
T +1 617 951 7495

Prudential Tower
800 Boylston Street
Boston, MA 02199



Deborah Gersh

deborah.gersh@ropesgray.com
T +1 312 845 1307

111 South Wacker Drive
46th Floor
Chicago, IL 60606

Timothy McCrystal

timothy.mccrystal@ropesgray.com
T +1 617 951 7278

Prudential Tower
800 Boylston Street
Boston, MA 02199

John Chesley

john.chesley@ropesgray.com
T +1 415 315 6394

Three Embarcadero Center
San Francisco, CA 94111

THE OCR AUDITORS ARE COMING - ARE YOU NEXT?

IDENTIFYING POTENTIAL VULNERABILITIES

By December 2012, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) plans to audit up to 150 covered entities. To help you and your organization prepare, our Health Care Privacy and Data Security attorneys have developed the following checklist.

If you answer "No" or "I Don't Know" to one or more of these questions, we encourage you to contact us to help your organization conduct a thorough assessment.

Technical Safeguards			
Wireless Access	Yes	No	I Don't Know
Do you have an effective encryption program (i.e. complying with the standards in HITECH)?			
Have you installed a wireless intrusion prevention system to prevent rogue wireless access points, and do you have a mechanism in place to monitor wireless network security?			
Do you have firewalls separating wireless networks from internal wired networks?			
Have you turned off automatic broadcast of service set identifiers so that they are not publicly accessible?			
Do you have effective authentication requirements for entering your wireless networks?			
Access Control	Yes	No	I Don't Know
Do you maintain strict access controls on domain controllers, servers, workstations, and mass storage media used to receive, maintain, or transmit Electronic Protected Health information ("ePHI")?			
Do you require adequate password settings for all password protected materials and databases, and do you require that all passwords are regularly changed?			
Have you enabled automatic user log off after periods of inactivity?			
Do you limit the number of unsuccessful log-on attempts before access is terminated, at least temporarily?			
Do you only allow use of encrypted laptops for access to or storage of ePHI?			
Do you limit user access to root folders?			

Access Control (cont.)	Yes	No	I Don't Know
Do you have policies in place to ensure immediate termination of access to your system for former employees and other personnel who may have previously had, but should no longer have access to your systems?			
Audit Control	Yes	No	I Don't Know
Do you keep current audit logging on servers, routers, firewalls, databases and wireless access points that contain or transmit ePHI?			
Do you archive these audit logs?			
Do your network administrators perform routine reviews of operating system and application audit logs and investigate any suspicious or malicious activity, including attempts to hack your networks or compromise the confidentiality and integrity of network ePHI?			
Integrity Control	Yes	No	I Don't Know
Have you installed system-wide security patches?			
Do you update antivirus software and scan engines regularly?			
Do you have service arrangements with operating system vendors to ensure proper maintenance and support?			
Do you regularly remove operating systems that are no longer supported by the manufacturer?			
Do you restrict internet access for hospital users, and do you have an acceptable internet use policy in place?			
Entity Authentication	Yes	No	I Don't Know
Do you prohibit sharing of administrator accounts?			
Do you ensure that default user identifications and passwords are changed after the first use?			
Do you have appropriate transmission security safeguards (e.g. prevent use of plain text remote administration tools, require use of e-mail encryption in certain circumstances, disable unnecessary and unsecure network services systems)?			
Physical Safeguards			
Facility access control	Yes	No	I Don't Know
Do you make sure that indoor windows and doors to rooms housing ePHI are secured and locked?			
Do you have other security measures in place to secure physical PHI (e.g., keycard access to storage areas, etc.)?			

Device and media control	Yes	No	I Don't Know
Do you have an inventory system in place to keep track of portable or removable devices?			
Do you have a policy in place that requires removal of ePHI from media prior to disposal, and do you document such removal when it occurs?			
Do you require password protection for all easily accessible computers?			
Do you have an effective encryption plan in place for computers, equipment and removable media containing ePHI?			
Administrative Safeguards			
Device and media control	Yes	No	I Don't Know
Do you have appropriate security management processes in place for your organization (e.g. regular risk assessments of information management systems)?			
Do you have appropriate security incident procedures to provide for an immediate and well-organized response in the event of any security incidents involving ePHI?			
Do you have adequate contingency plans in place to address disaster recovery, storage of back-up tapes, and network disruptions?			
Do you have proper procedures in place to ensure adequate contractual arrangements with all business associates?			
Do you have policies and procedures in place regarding removal and transport of ePHI?			
Have you conducted initial and follow-up training on your security policies and procedures, including updating your workforce regarding changes in the law?			

If you have questions about these issues or other topics related to health care privacy and data security, please contact your Ropes & Gray attorney or a member of the Health Care Privacy and Data Security team listed below:

Michele M. Garvin

michele.garvin@ropesgray.com
T +1 617 951 7495

Prudential Tower
800 Boylston Street
Boston, MA 02199

Deborah Gersh

deborah.gersh@ropesgray.com
T +1 312 845 1307

111 South Wacker Drive
46th Floor
Chicago, IL 60606

Timothy McCrystal

timothy.mccrystal@ropesgray.com
T +1 617 951 7278

Prudential Tower
800 Boylston Street
Boston, MA 02199

John Chesley

john.chesley@ropesgray.com
T +1 415 315 6394

Three Embarcadero Center
San Francisco, CA 94111