5 Insights for executives

Are you ready for a HIPAA audit?

Avoid getting the next million-dollar penalty

Of special interest to
Health care executives

Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA) includes the subsection known as the Health Information Technology for Economic and Clinical Health (HITECH) Act. In addition to its incentives for health care organizations to adopt electronic health records (EHRs), HITECH extended the scope of the HIPAA Privacy Rule and the Security Rule, increased penalties for failing to protect PHI and increased enforcement for violations of the Health Insurance Portability and Accountability Act (HIPAA).

On 25 January 2013, the Department of Health and Human Services (HHS), released its final omnibus rule relating to these requirements. Changes incorporated into the final rules include:

- More robust patient privacy protections
- New rights over health information for individuals
- Greater limitations on using personal health information for reasons not directly related to a patient's treatment or for payment of services
- Required accountability over service providers
- Increased diligence when assessing potential privacy or security breaches

In addition to issuing enhanced rules for privacy and security of personal health information, HITECH mandates HHS to provide for periodic audits of covered entities (CEs) to assess their compliance, not only with privacy and security rules, but also with breach notification standards.

In January 2012, the Office for Civil Rights (OCR) initiated a 12-month pilot program of proactive audits to assess CEs' compliance with HIPAA. The pilot audits resulted in a defined audit protocol and identified common compliance challenges. Based on statements by Leon Rodriguez, Director of OCR, this program will continue into the future. [1]

As such, health care payers, providers and clearing houses need to be prepared for a HIPAA audit. However, as the final omnibus rules outline, so too do business associates (BAs) and their subcontractors. These additional entities are also now subject to the same security and privacy regulations – and the same penalties for non-compliance – as CEs.

[1] Source: http://www.healthcareinfosecurity.com/hipaa-audits-next-phase-a-5397

CEs and BAs need to prepare for a world where audits are the norm, enforcement is inevitable and fines for non-compliance are costly.

1

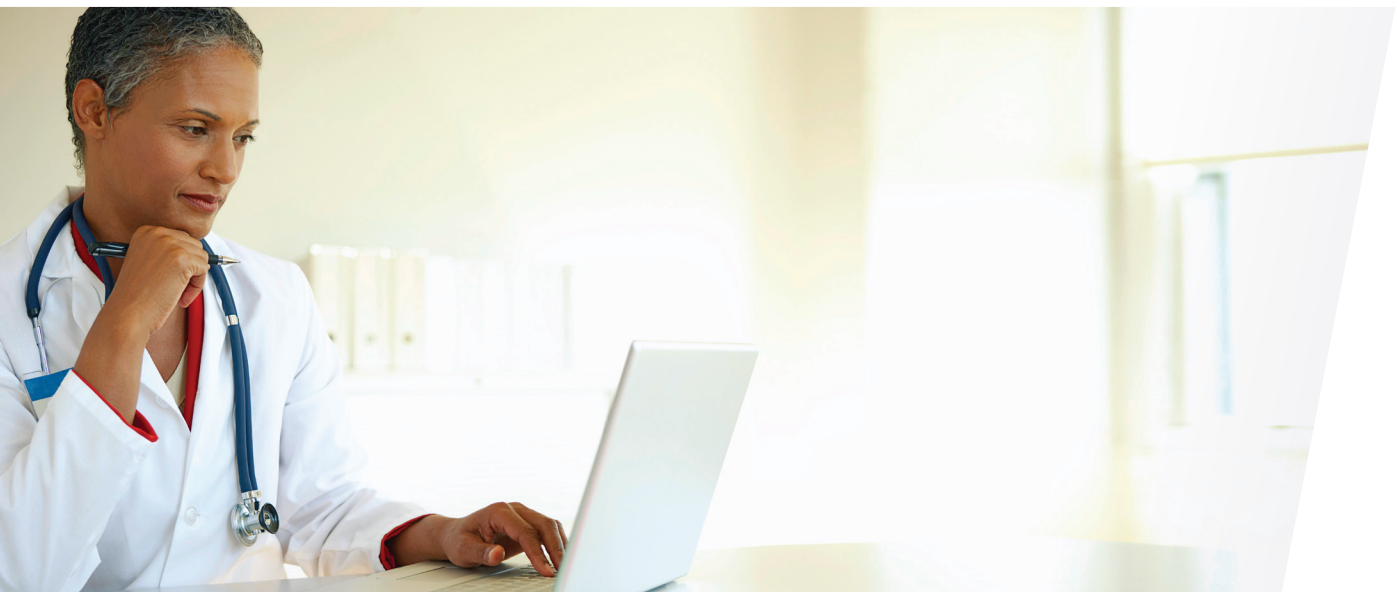
What's the issue?

Historically, HIPAA's enforcement was limited to events stemming from complaints, yet the associated civil penalties were often considered to be insufficient to convince CEs to adopt the rules. With the release of the final omnibus rule, there are clear indicators that suggest the enforcement landscape has changed:

- HITECH's Breach Notification Rule made privacy and security weaknesses publicly visible to the point where they cannot be ignored or dismissed.
- Enforcement totals for 2011 and 2012 were the highest ever and exceeded $10.8 million in fines.
- OCR's new director is an experienced prosecutor and has said the audits will become "a permanent and robust program." [2]
- HHS is authorized to use fines to fund further enforcement activities such as audits.

As OCR takes a more aggressive approach toward oversight and enforcement, CEs and BAs need to rethink their past approaches to HIPAA compliance. They need to prepare for a world where audits are the norm, enforcement is inevitable and fines for non-compliance are costly.

[2] Source: http://www.inforisktoday.com/permanent-hipaa-audit-program-coming-a-4253



A majority of CEs and BAs remain woefully unprepared to comply with the HIPAA privacy and security rules.

2

Why now?

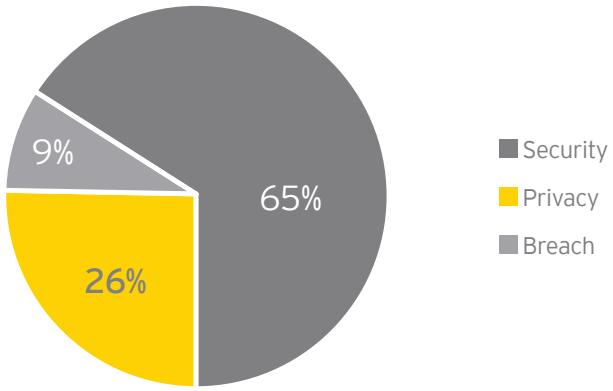
As the HHS makes its proactive HIPAA audit program permanent, a majority of CEs and BAs remain unprepared to comply with HIPAA privacy and security rules. Even CEs and BAs that have privacy and security programs in place don't feel confident that their programs will adequately demonstrate compliance with HIPAA.

In particular, CEs and BAs struggle to:

- Understand and reconcile the broad complexities of federal and state health care regulations
- Deal with limited and, in many cases, diminishing budgets to support the requisite personnel, IT controls and changes in business processes to meet HIPAA requirements
- Balance the organization's competing strategic initiatives of health care reform and health care compliance

Based on the pilot program audit findings released by the OCR, as well as information from organizations that have gone through the process, a majority of CEs audited had material issues noted. Almost two-thirds of the findings (65%) were related to the HIPAA security rule, 26% related to the privacy rule and the remaining 9% related to the HITECH breach notification rule.

Analysis of findings by rules



Source: 2012 HIPAA Privacy and Security Audits presentation

Although it will take substantial resources to effectively address these business risks, CEs and BAs can't afford to wait to improve their privacy and security programs and establish proactive readiness capabilities.

Under the new HITECH provisions, sanctions for non-compliance are substantial. They include new tiered fines, with a potential maximum of $1.5 million per identical violation per year.

3

How does it affect you?

Under the HITECH Act, state attorneys general can now bring civil actions to enforce HIPAA. Similarly, the Department of Justice is empowered to enforce HIPAA where criminal activity is suspected.

The following publicized actions of HHS and state attorneys general in response to a select number of HIPAA investigations that occurred in 2012 give CEs and BAs an idea of the risks they face if they do not improve their HIPAA privacy and security programs.

	Incident	Significance	HIPAA violation	Penalties
Phoenix Cardiac Surgery, P.C.	The physician practice was posting clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible	Demonstrates OCR's intent to vigorously enforce the HIPAA rules no matter the size of the covered entity	▸ Failing to implement adequate policies and procedures to appropriately safeguard patient information ▸ Failing to document that it trained any employees on its policies and procedures on the Privacy and Security Rules ▸ Failing to identify a security official and conduct a risk analysis ▸ Failing to obtain business associate agreements with Internet-based e-mail and calendar services where the provision of the service included storage of and access to its ePHI	▸ $100,000 settlement ▸ Corrective action plan to implement policies and procedures to safeguard the protected health information of its patients
Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. (MEEI)	Theft of an unencrypted laptop containing the ePHI of MEEI patients and research subjects	Fine of maximum penalty for "willful neglect"; agreement including mandatory corrective action plan	▸ Failing to conduct a thorough analysis of the risk to the confidentiality of ePHI maintained on portable devices ▸ Failing to implement security measures sufficient to ensure the confidentiality of ePHI ▸ Failing to adopt and implement policies and procedures to restrict access to ePHI to authorized users ▸ Failing to adopt and implement policies and procedures to address security incidents	▸ $1.5 million settlement ▸ Requirement for MEEI to adhere to a corrective action plan ▸ Consent to an independent monitor to conduct assessments of compliance with the corrective plan for three years
The Hospice of North Idaho (HONI)	Theft of laptop computer containing unencrypted ePHI	First settlement involving an ePHI breach affecting fewer than 500 individuals	▸ Failure to conduct a risk analysis to safeguard ePHI ▸ No policies or procedures in place to address mobile device security	▸ $50,000 settlement

4

What's the fix?

Although OCR has yet to announce a permanent audit program, one is on its way. To prepare, CEs and BAs should take the following actions:

1. Carry out or update the HIPAA risk analysis as required by the Security Rule, update the remediation plan and make progress toward remediating high-priority risks. CEs should also perform a gap analysis of the HIPAA safeguards and implementation specifications to better understand where they lack the necessary controls. Pilot audit results indicate risk analysis was ranked in the top five findings for audited CEs.
2. Establish a HIPAA audit response capability. CEs selected for audit have 15 days to respond to requests for information. CEs need to specify the responsive information control owners will have to provide in the event of audit. Examples of responsive information include:
   - Letters of designation for privacy and security officers
   - Evidence of how the physical, administrative and technical controls implemented to address HIPAA are operating
   - A copy of the preemption analysis for determining the most stringent provisions between HIPAA and other federal, state and local health care laws
   - Privacy and security policies, procedures and relevant forms
   - A copy of HIPAA training records
   - A sample of the current Notice of Privacy Practices, supplemented by archived versions
   - A copy of most recent internal privacy and security risk assessments, supplemented by archived versions
   - Copies of HIPAA program governance reports submitted to executive management
3. Leverage the publicly available results of the pilot audit program to benchmark the organization against the most common findings. The results suggest the following key areas of weakness exhibited by the CEs involved in the pilot:
   - User activity monitoring
   - Contingency planning
   - Authentication/integrity
   - Media reuse and destruction
   - Risk assessment

These recommendations assume that the organization already has an effective HIPAA governance structure in place to address the complexities of the regulations and the broad number of business and technology stakeholders required to support the program.

As OCR looks to make its pilot audit program permanent, now is the time for CEs and BAs to improve their privacy and security programs.

5

What's the bottom line?

Based on available information about the pilot HIPAA audit program, CEs and BAs face many hurdles in meeting their compliance obligations based on HIPAA's final omnibus rule. As OCR looks to make its pilot audit program permanent, now is the time for CEs and BAs to improve their privacy and security programs. The Ernst & Young HIPAA Acceleration Program Methodology provides a high-level framework for enhancing your HIPAA program. This approach has been implemented and tested at some of the largest, most complex covered entities.

Failure to meet the requirements of HIPAA and HITECH may result in hefty fines and lost revenue. More importantly, CEs and BAs may experience significant public embarrassment and brand damage, which can be much harder to overcome.

HIPAA acceleration program methodology

Phase	Goal and objective
1. Identify	Establish the HIPAA program and secure alignment of key business and technology stakeholders. Establish communications, reporting, governance, resource plans and project plans in order to define and achieve compliance objectives.
2. Diagnose	Perform risk analysis and control gap analysis to reveal areas of control weakness. Determine in-scope business processes including supporting systems, applications and data stores. Map the flow of PHI through business processes. Determine the controls to be implemented and prioritize key controls and systems based on risk. Create a "heat map" to define, monitor and communicate the highest risk areas.
3. Design	Design remediation activities to address the highest risks. Refine the work plan to determine priority and criticality of the applications and systems for remediation. Establish resource needs, plan remediation and mitigation efforts and architect solutions to address the control gaps.
4. Deliver	Execute the work plan to remediate risks identified in the applications, systems and key business processes. Deploy tactical teams in order to provide resources to stakeholders, where needed. Implement compliance sustainability tool – such as an enterprise GRC tool – to support ongoing compliance monitoring, testing and control attestations.
5. Sustain	Prepare HIPAA compliance readiness packages for regulatory inspection and internal audit review. Transition program to sustainable processes to be maintained by control and process owners facilitated through the implemented compliance and GRC tools. Periodically assess the program design and underlying control operating effectiveness to demonstrate compliance.

Want to learn more?

The answers in this issue are supplied by:

Reza Chapman
Senior Manager
Advisory Services
+1 602 369 4952
reza.chapman@ey.com

Justin Greis
Senior Manager
Advisory Services
+1 312 342 4202
justin.greis@ey.com

Glen Day
Senior Manager
Advisory Services
+1 805 778 7030
glen.day@ey.com

For related thought leadership, visit www.ey.com/5

We want to hear from you!

Please let us know if there are subjects you would like *5: insights for executives* to cover.

You can contact us at: fiveseries.team@ey.com

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 167,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About Ernst & Young's Advisory Services
The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 27,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver exceptional client service. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

© 2013 Ernst & Young LLP.
All Rights Reserved.

SCORE no. BT0265

ED None