The HIPAA Omnibus Rule

What You Should Know and Do as Enforcement Begins

Rebecca Fayed, Associate General Counsel and Privacy Officer

Eric Banks, Information Security Officer

Biographies

Rebecca C. Fayed is associate general counsel and privacy officer for The Advisory Board Company in Washington, DC. In this role, Rebecca advises on, and is responsible for all health regulatory and data privacy matters. Prior to joining the Advisory Board, Rebecca spent more than ten years as an attorney in private practice representing hospitals, health systems, health plans, health information technology companies, and other entities within the health care industry in connection with health regulatory and data privacy issues. Rebecca has extensive experience developing and implementing health information privacy and security compliance programs, and representing covered entities and business associates in connection with investigations related to privacy and security compliance and complying with federal and state breach notification obligations.

Eric Banks has been the Information Security Officer for The Advisory Board Company since July of 2010 and has over 17 years of combined experience in information security and IT leadership. His experience includes team development and project management within the health care, higher education, and human resources sectors, and he has been able to lead organizational change while continuing to manage complex technical projects. Eric is tied in to the information security community and is doggedly focused on proving that information security professionals, and the industry as a whole, can stretch beyond typical industry roles to help lead growth and add tremendous value throughout a company.

Learning Objectives

After attending this webinar, participants in this webinar will be able to:

1. Recognize how the HIPAA Omnibus Rule most significantly changed preexisting HIPAA privacy and security obligations.
2. Assess their privacy and security compliance programs against these new obligations.
3. Utilize industry best practices to supplement existing compliance programs.
4. Prepare for and respond to a potential breach, security incident, investigation, or audit.

The Omnibus Rule

Compliance Date:
September 23, 2013

What does the Omnibus Rule Do?

- ✓ Implements HITECH Act and certain GINA requirements
- ✓ Modifies HIPAA Privacy, Security, Breach Notification, and Enforcement Rules
- ✓ **Increases obligations, liability, and oversight/enforcement**
- ✓ **Creates a whole new HIPAA world**

Overview of the Most Significant Changes

Breach Notification Obligations	No more risk of harm?! But did anything REALLY change?
Business Associates	Who are they, what must they do, and what happens if they don't?
Use and Disclosure of PHI	Some expansion and some limitations
Individual Rights	Additional rights provided, but some questions left unanswered
Increased Oversight and Enforcement	The game changer

Breach Notification

Risk of Harm Was Always at Risk of Being Eliminated

Basic Rule Remains

Upon the discovery of a **Breach** of unsecured PHI, CEs and BAs must make certain notifications.

Breach

Unauthorized acquisition, access, use, or disclosure of unsecured PHI, in a manner not permitted by the Privacy Rule, that compromises the security or privacy of PHI (subject to certain exceptions).

Interim Final Rule (the "old" way):

Privacy or security of PHI was "compromised" if there was a significant risk of financial, reputational, or other harm to the individual affected.

Omnibus Rule

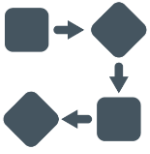
Not surprisingly, risk of harm eliminated from Breach analysis.

Risk Assessment is the New Standard

New Standard

Presumption

Impermissible acquisition, access, use, or disclosure **presumed** to be a Breach unless there is a **low probability that the PHI has been compromised.**



4 Factor Documented Risk Assessment

1. Nature and Extent of PHI involved
2. Unauthorized person who used the PHI or to whom PHI was disclosed
3. Whether PHI was actually acquired or viewed
4. Extent to which the risk to the PHI has been mitigated

Notification Obligations Remain the Same

Covered Entities

1. Notify the individuals affected without unreasonable delay, but within 60 days of discovery
2. If greater than 500 individuals affected **in total**, notify HHS of the breach at the same time individuals are notified
3. If less than 500 individuals affected **in total**, notify HHS of the breach within 60 days of the end of the calendar year in which the breach was discovered
4. If more than 500 individuals affected **in any given state**, notify prominent media outlets

Business Associates

1. Must notify the covered entity without unreasonable delay, but within 60 days of discovery.
2. Highly negotiated term of a BAA – how quickly must the BA notify the CE?

Business Associates

Same Actors, But Omnibus Rule Expanded the Definition

Confirmed What Many Already Believed to Be the Case

"Old" definition

Generally, a third party that provides certain services to a covered entity that involved "the use or disclosure" of PHI.

New Omnibus Rule Definition

1. Third party that provides certain services to a covered entity during which that third party "creates, receives, maintains, or transmits" PHI.

2. **Specifically includes:**
   - HIOs
   - E-prescribing gateways
   - Other providers of transmission services with routine access to PHI
   - PHR vendors engaged by CEs
   - A subcontractor that creates, receives, maintains, or transmits PHI on behalf of a business associate – **Creates a chain of BAAs all tied to the covered entity (but covered entities do NOT need BAAs with subcontractors)**

3. What about cloud computing providers?

4. What about third parties that only have access to encrypted data?

Additional Obligations

1

Breach Notification

2

Compliance with the HIPAA Security Rule

3

Compliance with use and disclosure provisions of the Privacy Rule, NOT the entire Privacy Rule

4

Best practices even if not legal obligations

Security Rule Changes

- ✓ Changes are more “conforming and procedural” than Privacy and Breach Notification Rules
- ✓ Conduit exception: check on Google Apps, DropBox, Skype
- ✓ Relationship between CE’s, BAs, and the BA’s BAs
- ✓ HHS expects that BAs were already meeting their obligations under HITECH and HIPAA
- ✓ Couldn’t be further from the truth!

BA Responsibilities Regarding the Security Rule

- ✓ Risk Management- Conducting risk analyses
- ✓ Policies and procedures
- ✓ Training
- ✓ Encryption analysis (is data in my database considered “at rest”?)
- ✓ Know your subcontractors!

Subcontractors and the Security Rule

A

Progressive/ Deep in Health

B

Large Industry Agnostic

C

Smaller Industry Agnostic

- ✓ Many smaller vendors that are now BA's are **not ready**
- ✓ Risk scoring with appropriate approvals for vendor analysis
- ✓ Don't be afraid to say no
- ✓ Be prepared to help them!

Increased Liability

Pre-Omnibus Rule:	**Omnibus Rule:**
• Breach of Contract	• Directly liable under HIPAA for violations of the Security Rule • Directly liable under HIPAA for impermissible use and disclosure of PHI under the Privacy Rule and/or under the BAA

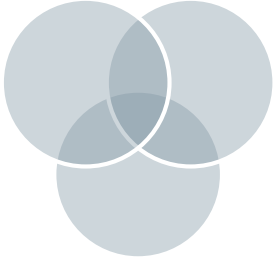
This was the game changer for business associates

Use and Disclosure of PHI

Use and Disclosure of PHI

Marketing

- Remuneration From a 3rd Party
- Refill Reminders
- Is anyone really surprised that marketing uses and disclosures were further restricted?



Fundraising

- New categories of PHI may be used or disclosed
- Right to opt-out strengthened

Sale of PHI

- Subject to certain exceptions, covered entities may not receive remuneration in exchange for PHI.
- Is anyone really surprised by this clarification?

Individual Rights

Individuals Have Additional Rights

Access to PHI

Electronic Copy of PHI

Restrictions on Use and Disclosure of PHI

Restrictions when item or service paid for out of pocket in full

Accounting of Disclosures

Many unanswered questions. Will access reports ever be required?

Increased Oversight and Enforcement

Increased Oversight and Enforcement

Remember January 2009, i.e., Pre-HITECH?

Little enforcement, little oversight, complaint-driven process?

It's Gone. For Good.

Post-HITECH

- Post- Breach Investigations
- Investigations of all cases of willful neglect
- Audits
- State AG Enforcement
- Complaint-driven process still alive and well too

Monetary Penalties are Higher

Think When, Not If

Compliance is Not Foolproof

1. Be prepared for a breach
2. Be prepared for a security incident
3. Be prepared for an investigation
4. Be prepared for an audit

What should you do now

Take Steps to Create a Culture of Compliance

- **Review, revise, and implement** policies and procedures
- **Develop** and conduct training
- **Set up process** and means for questions, incident reporting, etc.
- **Review and revise** business associate agreements
- **Assess business associates** and subcontractor compliance
- **Identify incident response team** and other responsible parties for security incidents, breaches, or other incidents **and have plan in place** to address these incidents.
- **Get senior leadership and board** on board with a culture of compliance

How Do I Assess My Company and Vendors For Security Rule Compliance?

- A good Risk Assessment is key
- Key areas are **Governance**, **Physical Security**, **Access Control**, **Data Storage and Transmission**, **Incident Response, Vulnerability Management, Network Security, Risk Management, DR/BCP, and Third-Party Oversight**
- You can use similar assessments for yourself, vendors, and partners
- Score your vendors and approve/reject based on that scoring

Security Action Items that Relate to Your Subcontractors

- **Create or enforce** your vendor risk assessment process
- **Ask vendors for their Risk Assessment** or external assessment results
- **Don't overlook vendor/partner applications** – are they secure?
- **If a subcontractor handles your PHI and doesn't know about the Omnibus Rule, be afraid**

What May the Government Ask For if You Have a Breach or Are Investigated?

- Clear documentation of the incident and facts surrounding the breach
- Copies of notification letters, media notices, business associate agreements
- Actions taken to locate missing data, prevent further loss of data, and protect affected individuals (e.g., credit monitoring services)
- Security Rule risk assessments
- Description of safeguards in place to protect the information, specifically requesting information related to whether data was encrypted and other documented safeguards
- Applicable Policies and Procedures and compliance efforts related to policies and procedure revisions, training, and sanctions imposed
- Your Incident Response and Employee Sanctions processes

Questions?

Rebecca Fayed
fayedr@advisory.com

Eric Banks
bankse@advisory.com