HIPAA Omnibus Rule: Is your organization ready for the compliance audits?

by Miguel O. Mercado, CISA

December 11, 2014
The information included in this presentation is for informational purposes only and is not provided as legal advice. The presenter is not a lawyer and provides this material as an overview of the key changes introduced in the HIPAA regulations as a result of the implementation of the Omnibus Rule. Examples are given only as current industry trends and do not constitute recommendations for action.
Health Insurance Portability and Accountability Act

HIPAA History

**1996**
- HIPAA—P.L. 104-191, Title II, Subtitle F – Administrative Simplification

**2002**
- Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164)
  - Published December 28, 2000 thru August 14, 2002;
  - Effective October 13, 2002;
  - Compliance April 14, 2003

**2003**
- Security Rule (45 CFR Part 160 and Subparts A and C of Part 164)
  - Published February 20, 2003;
  - Effective April 21, 2003;
  - Compliance April 20, 2005

**2006**
- Enforcement Rule (Subparts C, D and E of 45 CFR Part 160)
  - Published February 16, 2006;
  - Effective March 16, 2006

**2009**
  - ERM Implementation

**2013**
- Omnibus Rule
  - Published January 25, 2013
  - Effective March 26, 2013
  - Compliance September 23, 2013
  - Updates Privacy Rule
  - Updates Security Rule
  - Updates Enforcement Rule (including HITECH Act requirements)
  - Adds Breach Notification Rule (as required by HITECH Act)
Quotations from former HHS OCR Director
Mr. Leon Rodriguez:

“This final Omnibus Rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented.”

“These changes not only enhance a patient’s privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates.”
Health Information Privacy
Breaches Affecting 500 or More Individuals

Source: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
Heavily regulated industries tend to have a per capita data breach cost substantially above the overall mean of $201.
• HIPAA audits have increased in 2014.
• Department of Health and Human Services has made periodic HIPAA-related audits a focus in 2014 after running into funding issues in 2013.
What preparations should you make before HHS auditors shows up at your door?
What will HHS auditors look for?
How can I avoid surprises?
Is my organization ready?
Protected Health Information (PHI) - information that is a subset of health information, including demographic information collected from an individual, and that:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(a) Identifies the individual; or

(b) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
Covered Entity (Cover Entity) – one of the following which transmits HIPAA standard transactions electronically

- A health plan
- A health care clearinghouse
- A health care provider

Business Associate (Business Associate) – any individual or entity which creates, receives, maintains, or transmits PHI on behalf of a covered entity.
Omnibus – Privacy Rule Updates

- Business Associate (BA) definition expanded.
- Business Associates required to comply with certain parts of the Privacy Rule:
  - Business Associate is someone who “creates, receives, maintains, or transmits PHI on behalf of a Cover Entity”.
  - Applies even if contracted entity does not have access to actual view the PHI.
- Notice of Privacy Practices (NPP) requirements changed.
- Sale of PHI prohibited:
  - Can be done only with authorization.
- Marketing & Fundraising rules tightened.
• Patient has right to request restrictions under certain conditions.
• Patient has right to electronic access to their PHI.
• Genetic information now part the definition of PHI.
• Changes in protection of a decedent's health information – 50 years time frame.
• Immunization records may be disclosed when required to satisfy school admission (with parent’s consent).
Omnibus – Security Rules Updates

• Business Associates required to comply with the rule:
  – Business Associate Agreement (BAA) with Cover Entity must ensure Business Associate recognizes its obligation to comply with Security Rule.
  – Business Associate required to enter into a BAA with Subcontractors with same conditions as a Cover Entity to Business Associate.

• Patient’s right to restrict access needs to be recognized.

• Risk Analysis and Assessment (RAA) is a mandatory requirement.
• Penalties significantly raised:
  – Maximum $1,500,000 per calendar year for identical violations.

• Graduated scale based on Violation Category:
  – $100 - $50,000: Did not know and could not have known despite reasonable diligence.
  – $1,000 - $50,000: Reasonable cause but not willful neglect.
  – $10,000 - $50,000: Willful neglect but corrected within 30 days.
  – >$50,000: Willful neglect and not corrected when known.
Puerto Rico Hits Insurer with Record $6.8 Million Fine for HIPAA Breach

On February 18, Puerto Rican insurer Triple S Salud revealed that it will face a $6.8 million fine for violating the Health Insurance Portability and Accountability Act ("HIPAA"). According to an 8-K filing submitted to the Securities and Exchange Commission ("SEC"), the Puerto Rico Health Insurance Administration notified Triple S on February 11, 2014, regarding its plans to sanction the insurer for HIPAA violations resulting from a 2013 breach of protected health information. The Health Insurance Administration also plans to impose administrative sanctions on the insurer, including the suspension of new enrollments into one of its plans and the obligation to notify affected individuals of their right to disenroll.
Only OCR can decide if a set of violations are multiple instances of identical violation. Multiple maximum penalties may be caused by variations such as:

- Continuing over multiple days.
- Affecting multiple individuals.
- Violating multiple parts of the rule.

Cover Entity may be liable for penalty when violation is caused by a Business Associate.
Omnibus – Breach Notification Rule

- Final rule replaces interim rule of 2009.
- Implements strict guidelines on when and how a breach must be reported:
  - To the patient.
  - To the Secretary.
  - To the news media when case involves more than 500 patients.
- Business Associate responsible for reporting breach to Cover Entity.
- Cover Entity reports to patient and Secretary.
Understanding Roles

• Important to be clear in which role each party fits under HIPAA.
• While both Cover Entity's and Business Associates are now responsible directly, each incident will be evaluated.
• Cover Entity to Cover Entity:
  – Cover Entity may exchange PHI with another Cover Entity without holding one responsible to the other.
  – Each Cover Entity can assume the other is responsible under HIPAA
  – Minimum Necessary applies.
• Cover Entity to Business Associate:
  – Business Associate Agreement should exist.
  – Business Associate’s allowable uses of PHI must be spelled out.
  – A Cover Entity can be the Business Associate of another Cover Entity, depending on circumstances and actions performed.
  – Existence or lack of a Business Associate agreement is not the determinant of a Cover Entity-Business Associate relationship.
• Cover Entity to Business Associate (continued):
  – If OCR decides an entity is a Business Associate of a Cover Entity then it will be treated as such:
    • Business Associate will be held liable for HIPAA compliance.
    • Cover Entity will be guilty of non-compliance for failing to have a Business Associate Agreement in place (quite possibly this will be judged to be “Willful Neglect”).
  – Business Associates direct responsibility for compliance does not absolve Cover Entity of any responsibilities.
Business Associate to Business Associate:

- Subcontractors of Business Associates are now also Business Associates and responsible under HIPAA:
  - Cover Entity – Business Associate – Business Associate - . . . chain is unlimited
- If OCR decides an entity is a Business Associate of a Business Associate then it will be treated as such:
  - Subcontractor will be held liable for HIPAA compliance as a Business Associate.
  - Business Associate will be guilty of non-compliance for failing to have a Business Associate Agreement in place with the Subcontractor.
• HIPAA Privacy and Security policies and procedures need to be fully revised and brought up to date.
• Security incident response and management programs must be defined and established.
• Security breach notification policies and procedures should be put in place.
• A full assessment of Business Associate relationships should be conducted.
  – All existing relationships should be re-examined.
  – All Business Associate agreements should have been revised
  – All Business Associates should have been contacted and made aware of their status and responsibilities

• Procedures should have been implemented to evaluate all new relationships for Business Associate status.
Omnibus – Changes Needed (continued)

- Notice of Privacy Practices (NPP) must have been reviewed and updated:
  - Incorporate patient right to electronic access to PHI
  - Incorporate right to request restrictions.
  - NPP should be published in company website.
A full security risk analysis should be conducted:
- Mandatory requirement of the Security Rule.

Recognition of right of Patient to request restrictions on PHI:
- Specifically added absolute right to request restriction on PHI where information relates to health care for which the individual paid.
- Not easy to manage as it may apply to a particular service within an encounter.
• Recognize right of Patient to request electronic access to their PHI:
  – Patient can ask for access or a copy in electronic form of their choosing.
  – May only be denied if the Cover Entity can show it is not practical for them to create the format requested, then must negotiate with patient.
• Organization:
  – What type of HIPAA entity is your organization?
  – What type of HIPAA entity are your business partners?

• HIPAA Policies and Procedures:
  – Do they exist and have they been updated?
  – What changes to legal terms and conditions are required?
  – What changes will be required in the vendor management process?
  – Requiring contractors to recognize your policies is a problem if they cannot be given those policies.
  – Contractor’s attestation to following your policies is contradictory to being a Business Associate. Can either be part of workforce or be a Business Associate, but not both.
  – Workforce needs to be trained in policies and procedures and updated on them.
• eCFR HIPAA Rules.
• General Administrative Requirements – 45 CFR Part 160
  Enforcement Rule at Subparts C, D and E
  – http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=b3812134c1089175288d31a1157eeaf4&r=PART&n=45y1.0.1.3.75
• Privacy and Security – 45 CFR Part 164 Privacy Rule at
  Subpart E, Security Rule at Subpart C, and Breach Notification Rule at Subpart D
  – http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=b3812134c1089175288d31a1157eeaf4&r=PART&n=45y1.0.1.3.78
Our Management Team

Your Trusted Guide and Advisor

Miguel O. Mercado, CISA
Principal

- Mr. Mercado counts with 20 years of experience in the Financial Services, Insurance, Health Care and Public Sector industries. As the former Corporate Information Security Officer (CISO) of Puerto Rico’s largest financial institution Mr. Mercado was responsible for establishing and managing the organization information security and risk management programs as well as interacting with the Board of Directors, the organization Risk Management Committee and regulatory agencies in the oversight and risk management processes.

- Mr. Mercado brings years of practical experiences to each project. Mr. Mercado considers and integrates industry best practices in each engagement with the objective to implement effective and efficient processes and controls that can help reduce and manage key areas of risks for the organization in a cost effective way.

- Our mission is to help organizations increase the efficiency and effectiveness levels of its IT assets and investments by integrating a risk based approach to proactively identify areas that could impact the organization business objectives, projects and goals.

Contact:
E-Mail: miguel@baconpr.com
Tel. (787) 399-5010