eHEALTH INITIATIVE

Real Solutions. Better Health.

New HIPAA Rules and Implications for the Industry

January 29, 2013

**Audio for this webinar streams through the web. Please make sure the sound on your computer is turned on. If you need technical assistance, please contact ReadyTalk Customer Care: 800.843.9166.

eHEALTH INITIATIVE

Real Solutions. Better Health.

Jennifer Covich Bordenick

Chief Executive Officer

eHealth Initiative

Housekeeping Issues

- All participants are muted
  - To ask a question or make a comment, please submit via the chat feature and we will address as many as possible after the presentations.
- Audio and Visual is through www.readytalk.com
  - If you are experiencing technical difficulties accessing audio through the web, there will be a dial-in phone number displayed for you to call. In addition, if you have any challenges joining the conference or need technical assistance, please contact ReadyTalk Customer Care: 800.843.9166.
- Today's slides can be downloaded for free on our homepage at www.ehealthinitiative.org
- Today's webinar is being recorded
  - Members can access slides and replays of any webinar for free from eHI's store
  - Non-members can purchase access to any webinar replay for $25.00
  - eHI Store
    - http://www.ehealthinitiative.org/store.html

About eHealth Initiative

- Since 2001, eHealth Initiative is the only national, non-partisan group that represents all the stakeholders in health care.
- Mission to promote use of information and technology in healthcare to improve quality, safety and efficiency.
- Coalition of over 200 organizations and the most influential groups in data issues, HIT and HIE.
- eHealth Initiative focuses its ***research, education and advocacy*** efforts in four areas:
  - Using Data and Analytics to Understand and Improve Care
  - IT Infrastructure to Support Accountable Care
  - Technology for Patients with Chronic Disease
  - Connecting Communities through Data Exchange

eHealth Initiative's 2013 Annual Conference: Leading IT Forward

Join dozens of health IT executives, experts and innovators **February 12-13 at the Wyndham Orlando Resort in sunny Orlando, Florida**! The *eHealth Initiative's Annual Conference* features 35 national experts, interactive panels, best practices and case studies on

- The Opportunity of Technology & Big Data
- Using Analytics in Accountable Care
- Best Practices in Data Exchange
- A Patient's Perspective on Information Technology
- Current Health IT Practices in Accountable Care
- Applying the "Watson" SuperComputer to Healthcare Analytics
- Big Data to Solve Big Problems - Using Analytics for Population Health
- The New Congress: What It Means to Healthcare Policy Real World Use of Analytics
- Technology to Help Patients Manage Chronic Conditions

Thank You to Our Sponsor

pwc

Agenda

- Welcome – 2:00 p.m.
  - Jennifer Covich Bordenick, Chief Executive Officer, eHealth Initiative
- Understanding the Rule – 2:10 p.m.
  - Mick Coady, Principal, Health Information Privacy and Security Practice, PwC
- Top 10 List – 2:30 p.m.
  - James Koenig, CIPP, Director and Leader Privacy and Identity Theft Practice, PwC
- Questions and Answers – 2:50 p.m.
- Final Thoughts from Speakers and Closing – 3:25 p.m.

www.pwc.com

How to respond to the final omnibus HIPAA rule

10 Things You Need to Know Now

January 2013

On January 17, 2013, U.S. Department of Health and Human Services announced the final omnibus HIPAA rule that, among other things, enhances patient privacy protections, provides individuals new rights to their health information, and strengthens the government's enforcement of and penalties under the law.

While some of the changes alter the way organizations interact with patients and employees and use health data, organizations that simply address the new rules, without consideration of the many new privacy and security laws, risk creating their own patchwork of processes and controls that will ultimately prove less effective and unnecessarily expensive to build and maintain.

pwc

Our Speakers for Today

Mick Coady

Partner & Co-Leader, Health Information Privacy & Security Practice, PwC

mick.coady@us.pwc.con

Jim Koenig

Director & Co-Leader, Health Information Privacy & Security Practice, PwC

james.h.koenig@us.pwc.com

How to Respond to the Final Omnibus HIPAA Rule

A. Overview of the Final Omnibus HIPAA Rule
B. 10 Things You Need to Know Now

Overview of the Final Omnibus HIPAA Rule

Final Omnibus HIPAA Rule

On January 17, 2013, U.S. Department of Health and Human Services announced the final omnibus HIPAA rule that, among other things, enhances patient privacy protections, provides individuals new rights to their health information, and strengthens the government's enforcement of and penalties under the law. Effective date: 3/26/13 Compliance date: 9/23/13

What is the issue?

The final rule implements portions of the Health Information Technology for Economic and Clinical Health (HITECH) Act already in effect, but also includes modifications and requirements under HIPAA not previously included in the HITECH Act. Organizations that simply address the new provisions, without consideration of the many new privacy and security rules and regulations, risk creating their own patchwork of privacy and security processes and controls that will ultimately prove less effective and unnecessarily expensive to build and maintain.

Why it's important?

There is a revolution in health information and health IT -- moving toward EHRs, HIEs, ACOs, analytics, outcomes-based research, mobile, telemedicine, social media and other new and secondary uses. The new HIPAA changes will have immediate consequences, and the handling of health information is increasingly a regulated and complex area with heightened penalties and disclosure requirements for breaches and missteps. It is important for organizations to understand the financial and operational implications and develop a well thought out strategy to remain in compliance and support the new health information uses, health IT and channels.

Overview of the HIPAA Final Rules

Final HIPAA Rule Overview. The omnibus final rule strengthens and expands patient rights as well as enforcement and is comprised of the following four components:

1. **HIPAA Privacy, Security and Enforcement Rules and HITECH Act.** The final rule modifies the Privacy, Security, and Enforcement Rules. These modifications include:
   - changes regarding business associates;
   - limitations on the use and disclosure of PHI for marketing and fundraising;
   - prohibition on the sale of PHI without authorization;
   - expand rights to receive electronic copies of health information and to restrict disclosures to a health plan concerning treatment paid out of pocket in full;
   - requirement to modify and redistribute notice of privacy practices;
   - modify the individual authorization and other requirements to facilitate research, disclosure of child immunization proof to schools and access to decedent information by family members/others.
2. **Enforcement Rule.** Final rule adopts changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act.
3. **Breach Notification Rule.** Final rule adopts the Breach Notification for Unsecured PHI created under the HITECH Act, and replaces the breach notification rule's "harm" threshold with a more objective standard.
4. **HIPAA Privacy Rule as it Relates to Genetic Information.** Final rule modifies the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to increase privacy protections for genetic information by prohibiting most health plans from using or disclosing genetic information for underwriting purposes.

1. Modifications to Privacy, Security, and Enforcement Rules per HITECH

Area	Key Changes	Compliance Date
Business Associates		
Definition Expanded	• Expanded to include any entity that "creates, receives or transmits" PHI on behalf of a covered entity	Existing BA agreements not modified between March 26 and Sept. 23 remain compliant until earlier of either: 1) the date the agreement is renewed/modified on or after Sept. 23, 2013; or 2) Sept. 22, 2014
Subcontractors Included	• Definition now includes "subcontractors," patient safety organizations, e-prescribing gateways and vendors • Must conduct risk assessments	
Liability for BAAs and Subcontractors	• BAs are directly liable for impermissible uses/disclosures. • BA needs to have a BAA with any subcontractor creating, receiving, or transmitting PHI	
Hybrid Entities May Now Just Be CE	• Healthcare component for hybrid entities must now include all BA functions within the covered entity	
Conduit Exception Narrowed	• Exception only includes courier services that transport information (persistent vs. transient opportunity to access)	
PHR Vendors	• PHR vendors covered if services provided on behalf of a covered entity	

1. Modifications to Privacy, Security, and Enforcement Rules per HITECH (continued)

Area	Key Changes	Compliance Date
Sales, Marketing & Fundraising		
Sales and Marketing Communications	• Authorization required for treatments and communications where covered entity receives payment from a third party for a marketed product or service • Exceptions for refill reminders and communications about currently prescribed biologics	September 23, 2013
Fundraising	• NPPs must explain that an individual may be contacted to raise funds, but retains the right to opt-out	
Patient Rights		
Access to Receive Electronic Records	• Expands right to receive electronic copies of records	September 23, 2013
Research and School Immunization Rights; 50 Year Post-Death De-Classification	• Allows for compound authorizations and to include future uses of data for research • Modifies authorization to facilitate disclosure of child immunizations to schools • PHI protections cease 50 years from date of death	
Out of Pocket Services/Products	• Restricts disclosures to health plans for products/services paid for in full out of pocket	
Updated Notice of Privacy Practices	• Must provide updated NPP including right to be notified of breach, genetic information, out of pocket, research	

2. *Modifications to the Enforcement Rule*

Area	Data Points		Compliance Date
Tiered Civil Monetary Penalties	• **Increased and Tiered Civil Monetary Penalties.** Based on culpability, penalties now include:		September 23, 2013
	VIOLATION	EACH VIOLATION	
	Did not know	$100-$50,000 per violation ($1.5 million cap)	
	Reasonable Cause	$1,000-$50,000 ($1.5 million cap)	
	Willful neglect/corrected	$10,000-$50,000 ($1.5 million cap)	
	Willful neglect/uncorrected	$50,000 ($1.5 million cap)	

3. Modifications to the Breach Notification Rule

Area	Data Points	Compliance Date
Breach Notification for Breach of Unsecure Data	• **Automatic Presumption.** Impermissible use/access is presumed to be breach requiring notification unless risk assessment demonstrates otherwise • **Objective Standard.** Replaces "harm" threshold with "very little probability of PHI being compromised" standard	No later than 60 days from the discovery of the breach; HITECH requirements still in effect until September 23, 2013.
Post-Breach Risk Assessment of Very Little Probability	1. Nature and extent of PHI 2. To whom PHI may have been disclosed 3. Actual vs. possible 4. Mitigating factors	Performed routinely following security breaches and to comply with certain state notification laws; compliance date September 23, 2013

4. *Modifications to the Privacy Rule Based on Genetic Information Nondiscrimination Act (GINA)*

Area	Data Points	Compliance Date
Restriction on Using Genetic Information for Underwriting Purposes	• Prohibits most health plans from using or disclosing genetic information for underwriting (exception for long term care plans)	September 23, 2013
Family Information Included in Definition	• Genetic information includes genetic tests and individual's family health history	

How to respond to the Final Omnibus HIPAA Rule

A. Overview of the Final Omnibus HIPAA Rule
B. 10 Things You Need to Know Now

10 Things You Need to Know Now

- **Impact of the HIPAA Final Rules.** Any legal analysis of the final HIPAA rule will leave you with the impression that the privacy and breach notification provisions will require substantial operational changes for HIPAA-covered entities, their business associates and even subcontractors.

- **Changes Affect Entire Healthcare Industry.** Yet, there are numerous other US and global new privacy and data protection laws that impact HIPAA & non-HIPAA organizations. Also, health IT is undergoing considerable changes supporting new treatments and IT changes and health information uses.

- **10 Things to Consider.** In order to help structure your response to not only the final omnibus HIPAA rule, but also to the myriad of other recent privacy and data protection laws and standards, we are making 10 key suggestions that can be consider when planning the road forward.

10 Things You Need to Know Now

1. **The Stakes Have Changed. Communicate New Requirements, Need for Changes and Resources to Senior Management.**
   - Communicate that there are increased and tiered civil money penalties (Maximum: **$1.5 million** per incident). *Before HITECH: $100 per cap/violation, total cap of $25,000.*
   - Penalties apply to both BA's and subcontractors.
   - Hybrid entities must reassess legal status and if they need to enhance controls at BA functions within covered entity.

2. **BA's Are Treated As Covered Entities, Must Now Conduct Risk Assessment and Enhance Safeguards.**
   - Update/enter into BAAs - those entered into after 1/25/13 must be updated by 9/23/13.
   - BAs and subcontractors (no matter how far downstream) must comply with/are liable for violations under HIPAA Privacy/Security Rules. BAA must be entered into by BAs and subcontractors - must be similar to/stronger than BAA above it. Reassess conduits.
   - *BAs and subcontractors must assess reasonable, foreseeable risk to PHI.*

3. **Contractors, Including BA's, Are Assessing Vendor Practices, Compliance.**
   - Organizations are enhancing/expanding processes for vendor oversight (i.e. pre-contract assessments & post-contract audits).
   - Some subcontractors not previously subject to the HIPAA rule may face challenges complying before the compliance date of September 23, 2013.

10 Things You Need to Know Now (cont.)

4. Review Design & Functionality of EHR Systems to Address Requests for Records.

- Covered entities must provide an individual with access to PHI electronically if requested and *if* that data is maintained digitally.
- Covered entities continue to have 30 days to respond to requests for access to PHI. Covered entities may charge a fee for copies.

5. Update Notice of Privacy Practices and Redistribute to Patients/Individuals.

- Provisions of final rule must be reflected in Notice of Privacy Practices (NPP). NPPs must:
  - *notify individuals that they will be notified in the case of a breach*
  - *spell out disclosures, such as marketing and fundraising, that require authorization*
  - *specify that genetic information can not be disclosed to health plans for underwriting*
  - *specify restrictions on disclosures to health plans for products/services paid out of pocket*
- Health plans posting NPP on website must display changes by 9/23/13 **and** provide revised NPP in next annual billing to covered individuals (either at beginning of year or during open enrollment).
- Providers required to post copy of updated NPP and have copies on hand, while also providing NPP and obtaining acknowledgement from new patients.

10 Things You Need to Know Now (cont.)

6. Develop New Processes to Handle Modified PHI Use or Disclosure Requirements.

- Identify where genetic tests (and family history) is within organization. Develop processes to prevent disclosure to health plans for underwriting purposes (except long term care plans).
- Develop process to obtain authorizations for treatments and communications where covered entity receives payment from a third party whose product or service is marketed. (Exceptions: refill reminders and communications about currently prescriptions).
- *Revise informed consents/research authorizations to includes future uses of the data.*
- Assess situations where PHI is sold for fundraising purposes (unless fees are cost-based and reasonable).

7. Update Incident Response Plans to Address New Standards for Breach Notification.

- Companies need to revise incident response and breach notification processes to eliminate "harm" tests and include a conduct the 4 factor assessments of whether there is "very little probability of PHI being compromised."
- Importantly, HHS includes not just unauthorized access to PHI, but also impermissible uses by knowledgeable insiders as a breach requiring an assessment. This underscores the importance of ensuring strict data use controls and minimum necessary access controls.
- *HHS lifted a disclosure exception for limited data set. Now, certain research organizations who were once exempt are subject to the same compliance risks.*
- The HITECH breach notification law differs from most US state laws, as it includes breaches of health information and is not limited to electronic information.

10 Things You Need to Know Now (cont.)

8. Conduct a Data Element Inventory Beyond HIPAA for Compliance & Cost-Savings.

- Data element inventories are an effective means to locate PHI to determine where heightened safeguards and breach notification obligations apply to the now 19 HIPAA data elements.
- *With modifications to definition of PHI (e.g., genetic information, PHI 50 years after death), existing inventories may no longer be accurate, and organizations may need to update them.*
- Many companies are expanding data element inventory to cover the 60+ data elements specified in other federal, state and international laws.

9. Implement Encryption and/or Review Technologies and Data Classification Schemes Based on New Breach Notification and De-identification Requirements.

- HITECH established a federal security breach notification law for breaches of "unsecured" PHI. Many organizations have been preparing to secure or enhance security around PHI by:
  1. reviewing current encryption strategies
  2. updating data classification schemes
  3. implementing encryption and other technologies as appropriate
- Since HIPAA applies to both healthcare and human resources benefits data, many companies are adopting encryption that complies with NIST as the highest denominator
  - National Institute for Standards and Technology (NIST) SP 800-111 for data at rest
  - Federal Information Processing Standard (FIPS) 140-2, NIST SP 800-52, SP 800-77 and SP 800-113 for data in motion

10. Establish and Roll-Out an Integrated Privacy and Security Program Beyond HIPAA including (i) updated policy, NPP and procedure and (ii) training.

- Build an integrated privacy program that addresses not only HIPAA requirements but also includes key applicable US state, federal and global regulations.

Questions

To ask a question or make a comment, please submit via the chat feature.

Mick Coady

Partner & Co-Leader, Health Information Privacy & Security Practice, PwC

mick.coady@us.pwc.con

Jim Koenig

Director & Co-Leader, Health Information Privacy & Security Practice, PwC

james.h.koenig@us.pwc.com

(610) 246-4426

Final Thoughts

Mick Coady

Partner & Co-Leader, Health Information Privacy & Security Practice, PwC

mick.coady@us.pwc.con

Jim Koenig

Director & Co-Leader, Health Information Privacy & Security Practice, PwC

james.h.koenig@us.pwc.com

(610) 246-4426

THANK YOU TO OUR SPEAKERS!

Mick Coady
Partner & Co-Leader, Health Information Privacy & Security Practice, PwC
mick.coady@us.pwc.con

Jim Koenig
Director & Co-Leader, Health Information Privacy & Security Practice, PwC
james.h.koenig@us.pwc.com
(610) 246-4426

Thank You to Our Sponsor

pwc