Implications of HIPAA Requirements on Healthcare Payment Processing

Linda M Wolverton
Vice President, Compliance, TEAMHealth

Lynne Pearson
Vice President, National Healthcare Treasury Management
Fifth Third Bank

NACHA
The Electronic Payments Association

PAYMENTS 2013
April 21-24 | San Diego, CA
Your Presenters:

Lynne Person  
Vice President, National Healthcare Treasury Management  
Lynne has over 25 years of experience in the financial services industry addressing both corporate treasury needs as well as bank treasury technology solutions. She has been with Fifth Third for eight years and prior to that held positions with ACI, FIS and Harbinger. Roles have encompassed sales, marketing and product management in the treasury management field. Currently, Lynne works with national healthcare providers and payers in optimizing working capital through effective treasury solutions.

Linda Wolverton, CHC, CHPC, CPHQ, CHCQM, CPMSM, CPCS, RHIT, LHRM  
Vice President of Compliance  
Over 30 years of management level at TeamHealth and various other healthcare organizations. She is certified in Compliance, Healthcare Privacy Compliance, Health Information Management, Healthcare Quality, and Medical Staff Services. She is a Licensed Healthcare Risk Manager. She is on the Healthcare Compliance Associations Editorial Board, and also served 6 years in a senior position in the Health Care Compliance Association.

lynne.pearson@53.com  
Linda_Wolverton@teamhealth.com
Agenda

- HIPAA and HITECH/OMNIBUS fundamentals
- Regulatory implications on payments for FI’s, providers and payers
- Enforcement and legal actions
- What should healthcare clients and the FI be discussing
Process Evolution and the Resulting Rules = Complexity

Case 1

- I.M.A. Insurance Company mails Explanation of Benefits (EOBs), Remittance Advices (RA) and other documents to Good Partner Bank
- The delivered documents, EOBs, RAs and other documents, may contain
  - patient name
  - address
  - financial information
  - diagnosis (MS-DRG/CPT) or physician’s evaluation and management codes (CPT)
- The address on the envelope includes the client name – ABC Emergency Partners - and correct lockbox number
- The documents are placed in XYZ Hospital Medicine lockbox #123457, instead of ABC Emergency Partner’s lockbox #123456
- What would be your process?
Case 2

- I.M.A. Insurance Company mails Explanation of Benefits (EOBs), Remittance Advices (RA) and other documents to Good Partner Bank
- The address on the envelope includes the client name and lockbox number
- The delivered documents (EOBs, RAs and other documents) may contain patient name, address, financial information, and diagnosis (MS-DRG/CPT) or physician’s evaluation and management codes (CPT)
- The documents are placed in lock box number 123457 for ABC Emergency Partners’ lockbox, because the envelope was labeled with 123457
- However, the Good Partner Bank finds that the internal documents stated ‘XYZ Hospital Medicine’

What is your process?
Beyond the Lockbox

• How the Bank’s ‘Covered Entity’ or ‘Business Associate’ client thinks

  1. Was there was a patient identifier (account number, hospital, patient name, etc.)?
  2. Was there clinical information or financial information?
  3. Was this PHI and is this a HIPAA violation?

    –If the answer to 1 & 2 is yes, then
    –the answer to 3 is ‘perhaps’
Beyond the Lockbox: CCD+ versus CTX Considerations

- CCD+ will be the operating standard for healthcare claim payment EFTs *(NACHA rule effective 09.20.13, PPACA compliance deadline 01.01.14)*
- Under this standard no PHI is contained within the EFT
- CTX was not adopted as a standard due to the scale of change involved with current provider processes along with experience level
OK, what do those terms mean?

**Covered Entity**: is any organization or person who:
- Furnishes care
- Bills for that care
- Is Paid for health care in the normal course of business, and transmits health information electronically in connection with that care
  - Hospitals
  - Clinics
  - Clearinghouses
  - Physicians or a Provider of Care/’Provider’
Beyond the Lockbox

OK, a **Covered Entity** – is one who provides care and bills electronically

What is a **Business Associate**?

A Business Associate is a person or organization who handles PHI that belongs to a covered entity

- Healthcare billing company
- Banks with healthcare lockboxes
Beyond the Lockbox

• What is PHI - Protected Health Information
  1. Patient identifier (account number, hospital, patient name, etc.)
  2. Clinical information
     599.0 Urinary Tract Infection, site unspecified
     25500 Closed treatment of radial shaft fracture without manipulation
  3. Financial information
     Insurer paid $859.65
     Patient owes $20.00
November 21, 2011

ATTN: Billing Department
ABC Emergency Partners, Inc.
PO Box 123456
Upper Left Corner, TX

<table>
<thead>
<tr>
<th>Member Name:</th>
<th>Jane Doe</th>
<th>Date of Service:</th>
<th>9/1/2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member Number:</td>
<td>123</td>
<td>Total Charges:</td>
<td>$1,485.00</td>
</tr>
<tr>
<td>Group Number:</td>
<td>99999</td>
<td>Provider:</td>
<td>Pro Vider</td>
</tr>
<tr>
<td>Case Number:</td>
<td>123456789</td>
<td>Claim Number:</td>
<td>2345612345</td>
</tr>
</tbody>
</table>

Dear Billing Representative:

Thank you for your inquiry received in our office on November 23, 2011. You are requesting that IMA Insurance Company review the above listed claim for additional reimbursement.

This letter is to advise you that we did not review this as an appeal. After a review of Jane’s account, it was determined that this claim has already been reviewed as a Level II Appeal. IMA Insurance Company sent a response letter to Joe and your office on October 2, 2011 advising the claim processed correctly per the plan benefits.

If Jane does not agree, she can file a Level III Appeal. We cannot accept your request as a Level III without written release from Jane. The Level III Appeal should be received in our office no later than December 1, 2011 in order to be considered timely. I have included another Healthcare Release form for your convenience.

Thank you for the opportunity to provide you with this information. If you have any other questions, you may contact Customer Service at 555-555-5555.

Sincerely,

Jane Doe
Appeals Department

Example of what is PHI: identifier and financial information
2003 HIPAA and Personally Identifiable Information

• When care providers think of HIPAA what they almost always have in mind is the **Privacy Rule**

• The ‘Rule’ applies to **Covered Entities** and their use/disclosure of **Protected Health Information** (PHI)

**Basically:** protect patients’ protected health information (PHI) from those who have no need to know:

• For all disclosures, the covered entity is required to complete a disclosure log (**2003 Privacy Rule**). Patient name, address, what types of documents, to whom disclosed, and date of service are included.

→ No access / No disclosure
Personnel Identifiable Information – Red Flag Rules

2007- Sections 114 and 315 of the Fair and Accurate Credit Transactions act of 2003 or Red Flag Rule / Gramm-Leach-Bliley Act

- Financial institutions – State-Federal Banks, savings and loan associations, credit unions and mutual savings banks
- Creditors – finance companies, automobile dealers, mortgage brokers, utility companies. Telecommunications companies, 3rd part debt collectors, etc.
- **NOT Healthcare, Healthcare is excepted**
- Healthcare has policies to detect, prevent and mitigate, but are not bound by the Fair and Accurate Credit Transactions. We question the presenter of information and may, depending on circumstances, recommend notification of legal authorities.
2005 HIPAA Security Rule speaks only to protection of electronic PHI

Three standards:

1. **Administrative Safeguards** – policies which identify:
   - performance of security management process, assignment or delegation of security responsibility, training requirements, and.
   - evaluation and documentation of all decisions
   - who has access authorization, establishment, termination;
     a) Risk Analysis (Required)
     b) Risk Management (Required)
     c) Sanction Policy (Required) - deactivation
     d) Information System Activity Review (Required)

2005 HIPAA

2005 HIPAA Security Rule speaks only to protection of electronic PHI.
Three standards:

Physical Safeguards – Protection against inappropriate access – unauthorized intrusion, natural and environmental hazards, etc. Extends to workforce members homes or other physical locations where PHI may be accessed.

2005 HIPAA Security Rule speaks only to protection of electronic PHI.

Three standards:

Technical Safeguards

a) Unique User Identification (Required)
b) Emergency Access Procedure (Required)
c) Automatic Logoff (Addressable)
d) Encryption and Decryption (Addressable)

Requires a risk analysis and risk management processes

2009 HITECH Interim Rule

Health Information Technology for Economic and Clinical Health: ‘HITECH’ Interim Rule

Moves the 2003 Privacy Rule and the 2005 Security Rule into new territory:

1. Applies to Covered Entities and new to the HIPAA world: Business Associates (Banks, among others)
2. Fines and Penalties
3. Breach Notification
Health Information Technology for Economic and Clinical Health: ‘HITECH’ Interim Rule:

1. **Covered Entities** and **Business Associates** that access, maintain, retain, modify, record, store, destroy or otherwise hold, use, disclose unsecured PHI

2. Defines ‘**Breach**’ unauthorized access, use or disclosure of PHI which compromises the security or privacy of PHI

3. Breach, in 2009, had a risk assessment attached to it, which included: no ‘significant’ reputational, financial, or harm to the individual then, there was no breach; OR it met one of the exceptions
2009 HITECH Interim Rule

• All possible breaches/disclosures should be reported to your healthcare client: ASAP
  1. Federal regs - as soon as possible, due to the reporting requirement: **60 days from date of discovery to HHS report**
  2. California – ‘immediate’ is **within 5 days of date of discovery**

• All possible breaches may not be disclosures – example
  1. If the receiving lockbox is owned by the same organization as the lockbox where it should have been placed
  2. It may be minimum necessary rule that is violated

• Obtain a statement of confidentiality from the recipient, if possible

*This is NOT a ‘get out of jail card’, but assists in the risk reduction analysis*
• Penalties are tiered. Amounts may significantly increase penalties are based on the nature and extent of the harm resulting from the violation
  • Minimum penalty: $100
  • Maximum penalty: $1.5 million

Section 13410 (d) of the HITECH Act, eff 02-18-2009 revised section 1176 (a) of the SSA
Fines and Penalties

- The HITECH Act now allows states’ attorneys general to levy fines and seek attorneys fees from covered entities on behalf of victims
- Individuals now have liability
- Courts now have the ability to award costs, which they were previously unable to do

HCPro HIPAA and the HITECH Act: Know the level of penalties, HIM-HIPAA Insider, March 16, 2009
News Release

FOR IMMEDIATE RELEASE
March 13, 2012

HHS settles HIPAA case with BCBST for $1.5 million

First enforcement action resulting from HITECH Breach Notification Rule

Blue Cross Blue Shield of Tennessee (BCBST) has agreed to pay the U.S. Department of Health and Human Services (HHS) $1,500,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, Leon Rodriguez, Director of the HHS Office for Civil Rights (OCR), announced today. BCBST has also agreed to a corrective action plan to address gaps in its HIPAA compliance program. The enforcement action is the first resulting from a breach report required by the Health Information Technology for Economic and Clinical Health (HITECH) Act Breach Notification Rule.

The investigation followed a notice submitted by BCBST to OCR reporting that 57 unencrypted computer hard drives were stolen from a leased facility in Tennessee. The drives contained the protected health information (PHI) of over 1 million individuals, including member names, social security numbers, diagnosis codes, dates of birth, and health plan identification numbers. OCR’s investigation indicated BCBST failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes. In addition, the investigation showed a failure to implement appropriate physical safeguards by not having adequate facility access controls; both of these safeguards are required by the HIPAA Security Rule.

"This settlement sends an important message that OCR expects health plans and health care providers to have in place a carefully designed, delivered, and monitored HIPAA compliance program," said OCR Director Leon Rodriguez. "The HITECH Breach Notification Rule is an important enforcement tool and OCR will continue to vigorously protect patients’ right to private and secure health information."

In addition to the $1,500,000 settlement, the agreement requires BCBST to review, revise, and maintain its Privacy and Security policies and procedures, to conduct regular and robust trainings for all BCBST employees covering employee responsibilities under HIPAA, and to perform monitor reviews to ensure BCBST compliance with the corrective action plan.

HHS Office for Civil Rights enforces the HIPAA Privacy and Security Rules. The HIPAA Privacy Rule gives individuals rights over their protected health information and sets rules and limits on who can look at and receive that health information. The HIPAA Security Rule protects health information in electronic form by requiring entities covered by HIPAA to use physical, technical, and administrative safeguards to ensure that electronic protected health information remains private and secure.

The HITECH Breach Notification Rule requires covered entities to report an impermissible use or disclosure of protected health information, or a "breach," of 500 individuals or more to OCR. Smaller breaches affecting less than 500 individuals must be reported to the Secretary on an annual basis.

Individuals who believe that a covered entity has violated their (or someone else’s) health information privacy rights or committed another violation of the HIPAA Privacy or Security Rule may file a complaint with OCR at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

The HHS Resolution Agreement can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/resolution_agreement_and_csp.pdf.

Additional information about OCR’s enforcement activities can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

###

Note: All HHS press releases, fact sheets and other press materials are available at http://www.hhs.gov/news.
2009 HITECH Interim Final Rule

FINES AND PENALTIES

First HITECH Resolution Agreement Costs Insurer $17M

Hot off the Press – March 2012

- 57 unencrypted hard drives stolen from secured storage closet
- More than 1 million patients had detailed PHI data breached
- BCBST cited for failure to implement appropriate safeguards
- Updated security analysis not performed in response to office relocation activity
- Breach cost: $1.5M settlement + $17M breach response and corrective action

HHS.gov US Department of Health and Human Services March 13, 2012
2013 Final Omnibus HIPAA Rule

- Effective date: March 26, 2013
- Compliance Date: September 23, 2013 with some business associate agreement exceptions
- Final rule covers:
  1. Marketing and the use of PHI
  2. Sale of PHI
  3. Changes to PHI Access Policies
  4. Changes to Patient’s Right to Restrict Certain disclosures
  5. Changes to Policies related to Breach Reporting
  6. Revision of Notice of Privacy Practices
  7. Revision to Business Associate Agreements
#5 Changes to Policies related to Breach Reporting

Assumption that an Incident is Reportable

- Burden of Proof rests with the Covered Entity
- The healthcare entity will wish to perform the risk assessment:
  1) Increased diligence in the assessment
  2) More documentation in the assessment
  3) Incidents handled proactively to prevent mis-statements

Notify Covered Entity as Soon as Possible
#7 Revision to Business Associate Agreements

- Effective date: **March 26, 2013**
- Compliance Date: September 23, 2013 with some business associate agreement exceptions
- Definitions clarified:
  - A service provider that provides storage of PHI is considered a Business Associate
  - Downstream entities that work at the direction or on behalf of a Business Associate are required to comply with the Privacy and Security Rules (e.g. a shredding company)
If Business arrangement is:

1. currently operating pursuant to a compliant BA agreement in effect on January 2, 2013 and

2. the contract is not scheduled to be renewed or modified between March 26, 2013 and September 23, 2013

3. You are deemed in compliance, until

   a. Date that the contract or other arrangement is renewed or modified on or after September 23, 2013; OR

   b. No Later than September 23, 2014
2013 Final Omnibus HIPAA Rule

Revisions to Business Associate Agreements

• Reflect requirements of compliance with the 2005 HIPAA security rule

• Reflect need to report breaches

• Reflect need to have agreements with subcontractors.

Business Associates need BA agreements with subcontractors
2013 Final Omnibus HIPAA Rule

Effective date: **March 26, 2013**

Business Associates are required to:

- Limits uses and disclosures
- Comply with minimum necessary standards
- Provide breach notification to covered entity
- Provide a copy of the electronic PHI to covered entity / representative – as specified in agreement
- Disclose PHI to the Secretary of HHS in an investigation
- Provide an accounting of disclosures
- Comply with the 2005 security rule
## BOTTOM LINE – 4 Tiers of Penalties

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>Maximum for All Such Violations of an Identical Provision in a Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(B) Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(C)(i) Willful Neglect</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(C)(ii) Willful Neglect-Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
2013 Final Omnibus HIPAA Rule
What affects you?

500 disclosures:
• Business Associate is required to notify the Covered Entity
• Covered Entity has an Immediate Patient Notification/HHS/Media Reporting-immediate is defined as 60 days*

Date of Discovery (DOD) + 60 days to report to HHS, Media and notify patients

Example:
If the DOD is 01-01-13
Bank notifies the Covered Entity 01-20-12
Covered Entity has 40 days to:
• Investigate
• Correct any internal problems
• Write/mail notification letters
• Notify HHS of matter
• Notify the Media

*Except California -5 business days
Take-aways – Operational Structure

1. Determine eligible current or planned services and the financial institution’s status as a covered entity or business associate under HIPAA and HITECH

2. Set-up the infrastructure to successfully achieve compliance. This includes selection of:
   • Corporate level program sponsor
   • Privacy and Security officer.
   • These roles may be assumed by one or more individuals

3. Conduct
   • Risk analysis – electronic and paper
   • Risk Audit
   • Identify controls or control gaps

4. Review and update technology systems as needed

5. Develop a communications plan

6. Update workforce training

7. Consider data privacy and security accreditation or certification by independent third party such as EHNAC or HIMSS

Take-aways – Client Relationship and Process

What’s my take away?

- Contact the healthcare client’s Privacy or Compliance Officer to develop a working relationship and determine your clients needs
- Read your new Business Associate Agreement
- Immediate notification to your healthcare client of any disclosures with name of party and document examples
- Count the number of disclosures and share with the covered entity
- Notify the Covered Entity of the name(s) of the states – if possible
QUESTIONS?

Linda M Wolverton  
Vice President, Compliance, TEAMHealth

Lynne Pearson  
Vice President, National Healthcare Treasury Management  
Fifth Third Bank
The HIPAA Privacy Rule is contained in Subpart E (Privacy of Individually Identifiable Information) of CFR §164. Subpart E extends from § 164.500 through 164.534


HIPAA Security Rule February 20, 2003. It took effect on April 21, 2003 with a compliance date of April 21, 2005

Health Information Technology for Economic and Clinical Health (HITECH) Act Title XII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L.111-5)


HCPro – HIPAA and the HITECH Act: Know the level of penalties, March 16, 2009


https://www.nacha.org/c/newresources.cfm/AID/829