Assessing and Mitigating Risk Under the HIPAA Omnibus Rule

Darrell W. Contreras, Esq., LHRM, CHPC, CHC, CHRC
Chief Legal & Compliance Officer
PlusDelta Technologies, LLC

Agenda

- Omnibus Rule – Critical Elements
  - Disclosures to Health Plans
  - Business Associates
  - Breach Notification
- Addressing Risk
- Assessing Risk
  - Risk Assessment Documents
- Mitigating Risk
  - Corrective Action Plans
- Monitoring
- Summary/Q & A
HIPAA Omnibus Rule - Changes

- Business Associates and subcontractors
- Breach notification
- Marketing
- Sale of PHI
- Fundraising
- Notice of Privacy Practices
- Individual access to ePHI
- Third party designation for receipt of PHI
- Research
- Decedent PHI
- Student Immunization Records
- Restriction on health plan disclosures

Review of Critical Elements

Restrictions on Health Plan Disclosures:

- New Rule – Patients may restrict information provided to health plans if:
  1. If the patient requests the restriction;
  2. The patient has paid in full for the service or healthcare item;
  3. The disclosure would have been for payment or healthcare operations and is not required by law.
Application – Breach Notification Requirements

The Challenges of Restrictions on Disclosures to Health Plans:

- How do you flag requests?
- Are staff trained on how to respond to requests?
- Does your record system have a mechanism to flag these disclosures?

Review of Critical Elements

Business Associates and Subcontractors:

- “Maintains” now included in the definition of Business Associate
  - Anyone who stores PHI, even if it is not accessed, is a BA
- Privacy protection requirements are now extended to subcontractors of business associates
- All Business Associates must comply with the Security Rule requirements for safeguards:
  - Administrative
  - Physical
  - Technical
- BAs now have Civil and Criminal liability
- Covered Entities are responsible for breaches of BAs through “Agency Liability”
Application – Business Associate Agreements

The Impact of BA Changes to Covered Entities:

• The Covered Entities (CE) does not need a BAA with a subcontractor
  - The BA must have a BAA with the subcontractor
  - The subcontractor must agree to the same restrictions and conditions as the BA

• CE s should:
  - Revise their BAA to require subcontractor compliance
  - Obtain assurances (in the BAA) that the BA monitors compliance by the subcontractor
  - Consider indemnification clause in the BAA
    - CE s are responsible no matter what...try to protect yourself

Review of Critical Elements

Breach Notification Rules:

• Old Rule – A reportable breach occurs if 3 elements are present:
  1. Violation of the Privacy Regulations
  2. Unsecured PHI
  3. Substantial risk of financial, reputational, or other harm to the individual

• New Rule – A reportable breach is **PRESUMED** to have occurred if:
  1. There is a violation of the Privacy Regulations that includes
  2. Unsecured PHI

Unless ... “low probability” that PHI has been compromised
Review of Critical Elements

Breach Notification (Continued):

- “Low Probability” is based on 4 factors:
  - What was the nature and extent of the protected health information (PHI) involved, including the types of identifiers in the information and the likelihood of re-identification?
  - To whom was the unauthorized information disclosed?
  - Was the PHI actually acquired or viewed?
  - What was the extent to which the risk to PHI has been mitigated?

Application – Breach Notification Requirements

The Impact of Breach Notification changes:

- Change your risk assessment to evaluate the 4 factors
- As a practical matter...
  - The outcome of your assessment may not change
  - Obtain assurances (in the BAA) that the BA monitors compliance by the subcontractor
  - Consider indemnification clause in the BAA
    - CEs are responsible no matter what...try to protect yourself
Addressing Risk

Assessing Risk – Required by the Security Regs:
• Conduct an accurate and thorough assessment of the potential risks and vulnerabilities...of [ePHI]” 45 CFR 164.308(a)(ii)(A)

Mitigating Risk – Required... by the Security Regs:
• Security Regs: “...(mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity;” 45 CFR 164.308(a)(6)(ii)
• Privacy Regs: A covered entity must mitigate...any harmful effect that is known to the covered entity of a use or disclosure of [PHI]...” 45 CFR 164.530(f)

Addressing Risk

Monitoring Risk – Compliance Program Guidance:
• An ongoing evaluation process is critical to a successful compliance program. The OIG believes that an effective program should incorporate thorough monitoring of its implementation and regular reporting to senior hospital or corporate officers. (Compliance Program Guidance for Hospitals, Section F)
Disclosures to Health Plans

- Are we assessing, mitigating, or monitoring?
  - Step 1: Assess the process
  - Step 2: Identify deficiencies
  - Step 3: Develop corrective action
  - Step 4: Report completion of corrective action
  - Step 5: Monitor/Test the new process

Disclosures to Health Plans

- Look at Risk Assessment Document:

<table>
<thead>
<tr>
<th>Risk Area:</th>
<th>Patient request for restriction on PHI disclosed to health plans.</th>
</tr>
</thead>
</table>
| Description: | Under the HIPAA Omnibus Rule, a patient may request that a covered entity restrict the information that is provided to a health plan IF 3 conditions are satisfied:  
  1. The patient specifically requests the restriction of PHI;  
  2. The patient has paid in full for the restricted services; and  
  3. The disclosure to the health plan would otherwise be permitted for payment or health care operations. |

- Who completes this document?
- What level of detail is required?
- What is the purpose of this document?
Disclosures to Health Plans

• For our purposes, assume a process is in place...now what?
  ○ Testing – Depends on the level of risk
  ○ Mitigation?
  ○ Monitoring?

Disclosures to Health Plans

• Assume there is no process because, “We can’t track it”:  
  ○ Who’s job is this?  
  ○ What is your role in this?  
• Don’t forget the practical...  
  ○ How often does this happen?
Business Associate Agreements/Subcontractors

- Are we assessing, mitigating, or monitoring?
- Look at the Risk Assessment document:

<table>
<thead>
<tr>
<th>Risk Area:</th>
<th>Extension of BAA to subcontractors of business associates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>The HIPAA Omnibus Rule extended to covered entities liability for uses and disclosures of PHI by subcontractors of business associates. Business associates must obtain reasonable assurances from all subcontractors that use, disclose, receive, transmit, or store PHI that privacy and security protections have been implemented.</td>
</tr>
</tbody>
</table>

Business Associate Agreements/Subcontractors

- Look at the Business Associate Disclosure Form
- Who’s responsibility is this?
- What is your role?
- What is the next step?
Business Associate Agreements/Subcontractors

- If no list or no confidence of subcontractor compliance...
  - Mitigation
    - Audit/Test
      - Sample of contracts – both BAA and non-BAA
      - Follow-up with Business Associates
      - Make sure there is a process
  - Monitor
    - Annual Sample testing

- Don’t forget WHY?

Breach Notification

Breach Notification has 2 components:
1. Process in place for breach notification
2. Methodology to avoid breaches

Avoid = Assess, then Mitigate

How do you avoid a breach?
- Know how a breach could occur:
  - PHI leaving the organization
Breach Notification

Breach Notification has 2 components:
1. Process in place for breach notification
2. Methodology to avoid breaches

Avoid = Assess, then Mitigate
How do you avoid a breach?
• Know how a breach could occur:
  o PHI leaving the organization

• Risk areas for data to leave the organization:
  o Employees
  o Jump Drives
  o Hard Drives
  o Copies
  o Fax Machines
  o Misdirected VPN
  o Laptops
  o CD/DVD
  o External Storage
  o Paper Records
  o e-mail
  o Hacking/Intrustion
### Media Re-Use and Disposal

- **Look at Risk Assessment for hard drives**

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Media Re-Use and Disposal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Media that is no longer in use but contains PHI must be destroyed or the retained data rendered unusable.</td>
</tr>
</tbody>
</table>

### Media Re-Use and Disposal

- **Is this automatically a problem?**
- **What happens if it is?**
  - Who’s job is it?
  - What is your role?
    - Provide the standard/Policy Development
    - Identify the risk
    - Quantify the risk
    - Request updates
    - Report