Beyond The Legal Requirements: Key Practical Issues in Negotiating Business Associate Agreements, Responding to a Breach of Unsecured PHI, and Understanding HHS Enforcement

Philip L. Gordon, Esq.
Littler Mendelson, P.C.
Philip L. Gordon, Esq.
Littler Mendelson, P.C.
303.362.2858
pgordon@littler.com

Visit Littler’s Practice Group blog:
www.workplaceprivacycounsel.com
New Rules for Business Associates and Business Associate Agreements

Are you a BA?

KNOW THE RULES!
**Who Is A Business Associate?**

Third party that “creates, receives, maintains, or transmits protected health information” to perform:

<table>
<thead>
<tr>
<th>Services for a Covered Entity</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Claims Processing</td>
<td>Administration</td>
</tr>
<tr>
<td>Data Analysis</td>
<td>Processing or Administration</td>
</tr>
<tr>
<td>Utilization Review</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>Patient Safety</td>
<td>Billing</td>
</tr>
<tr>
<td>Benefit Management</td>
<td>Practice Management</td>
</tr>
<tr>
<td>Repricing</td>
<td></td>
</tr>
</tbody>
</table>
### Who Is A Business Associate?

Third party to whom a covered entity discloses PHI to provide the following types of services:

<table>
<thead>
<tr>
<th>Legal</th>
<th>Actuarial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting</td>
<td>Consulting</td>
</tr>
<tr>
<td>Data Aggregation</td>
<td>Management</td>
</tr>
<tr>
<td>Administration</td>
<td>Accreditation</td>
</tr>
<tr>
<td>Financial Services</td>
<td></td>
</tr>
</tbody>
</table>
1. **Subcontractors**: a person to whom a business associate delegates a function, activity, or service which involves creating, receiving, maintaining, or transmitting PHI

   **Example**: Third-party administrator retains a company to recover overpayments of benefits from plan participants

2. **Cloud Service Providers**: Document storage companies maintaining PHI on behalf of covered entities, regardless of whether they actually view the information they hold

   **Example**: Cloud computing services, such as Dropbox
3. **PHR Providers**: Entities that offer a personal health record to one or more individuals on behalf of a covered entity

   “Personal health record” = an electronic record of individually identifiable health information that can be drawn from multiple sources and that is controlled by the individual

4. **Health Information Exchange Organizations**: Provide data transmission of PHI to a covered entity

   **Example**: E-prescribing gateways
Some “Non-Obvious” Business Associates

- Document destruction companies
- Photocopy/scanning vendors
- IT vendors who provide services involving PHI
- Computer equipment repair services
- Translation/interpreter services
- Private investigators
Who Is Not A Business Associate?

- The “hand washing video” provider
- IT security and financial auditors who do not have access to PHI to perform their work
- Employment lawyers who do not receive PHI
- Internet service providers and other telecommunications providers
- Courier services
1. **What is your organization’s position in the negotiations: covered entity, business associate, subcontractor?**
   - First-tier business associates must enter into business associate agreements with subcontractors
   - Subcontractors must agree to enter into business associate agreements with their subcontractors

2. **What is your organization’s economic/financial leverage vis-à-vis the other party?**

3. **Is the underlying service agreement already in place, or is the BAA being negotiated after the service agreement has been executed?**

4. **Whose template are you starting with?**

5. **Does the template include all language required by the Privacy Rule?**
Mandatory Revisions to BAAs

Business associate agreements must be amended on or before 9/22/14 to impose the following duties on business associates:

1. Limit uses and disclosures of PHI to be consistent with the covered entity’s minimum necessary policies and procedures

2. Implement safeguards for electronic PHI in accordance with the HIPAA Security Rule

3. Notify the covered entity of a security breach
Mandatory Revisions to BAAs

4. Enter into a similarly restrictive business associate agreement with subcontractors

5. Fulfill any privacy obligation delegated by the covered entity in compliance with the Privacy Rule
Safeguards For PHI

Varying levels of detail can be proposed:

1. Parrot the language in the Privacy and Security Rule, *i.e.*, general reference to reasonable and appropriate safeguards

2. Reference by citation the specific sections of the Security Rule, *i.e.*, 45 C.F.R. pt. 164.308 (administrative safeguards); 45 C.F.R. pt. 164.310 (physical safeguards); 45 C.F.R. pt. 164.312 (technical safeguards)

3. Identify specific, required safeguards: (a) 24/7 video surveillance, (b) password requirements, (c) isolate PHI from the Internet, (d) 24/7 intrusion detection with maximum 15 minute response time, (e) encryption of portable devices
Related “Safeguards”

**Background Checks**
- Representation and warranty that they are performed
- Establish specific criteria, *i.e.*, no felony conviction in preceding seven years
- Retention and audit requirement

**Security Incident Response Plan**
- Expressly require the vendor to have one
Reporting A Security Event

What must be reported?

• Use or disclosure of PHI in violation of the BAA – Required by the Privacy Rule
• “Security Incident” – How to address “attempted” security incidents?
• “Breach of Unsecured PHI” – Who decides whether a security even is a “Breach”?

When must the Security Event be reported?

• Initial report: Range between 24 hours and 10 business days after discovery
• Follow-Up Report: 3 to 10 business days after initial report
Content Of “BAA Notice”

1. Minimum regulatory requirement: identification of affected individuals plus any other information needed by covered entity to prepare the notice to individuals

2. Specify all categories of information that the covered entity must include in its notice to individuals

3. Add other categories: (a) identification of specific contact at the business associate, (b) identification of law enforcement contacted, (c) last known mailing address of affected individuals, (d) the types of PHI compromised for each individual, if different

4. Require updates when material, new information becomes available
Control of Notification Process

1. Who will ultimately decide whether individuals will be notified?
2. Who controls the content of the notice?
3. Who decides which vendors will be used to support the notification process?
4. Who decides which products or services to offer affected individuals?
5. Who notifies the media? Who controls the content?
6. Who will notify HHS?
Allocation of Cost

Reimbursement Of Costs:
- All costs related to notification
- All costs related to services offered to individuals
- Imputed costs?
- Limit to “legally required” costs?

Limitations On Liability
- Check for limitation in underlying agreement
- If too low, provide that the limitation does not apply

Indemnification
- Is indemnification in underlying agreement adequate?
- All damages arising from Security Event or limited to business associate’s acts or omissions
Other “Optional” Provisions

1. Information security audits
   • Notice, frequency, scope, allocation of cost, confidentiality

2. Cyber-risk insurance
   • Scope of coverage
   • Amount of coverage per incident
   • Annual aggregate dollar limits

3. Return Or Destruction Of PHI
   • Who decides whether return or destruction is infeasible?
   • Certification of proper destruction
   • Carve outs: Back-ups, PHI retained for “legal reasons”
Responding to a Data Breach
Planning For A Breach

6 Key Steps For Advanced Preparation:
1. Evaluate cyber-risk insurance
2. Identify and engage “breach counsel”
3. Identify and engage incident response vendors
   – Computer forensic investigators
   – Credit monitoring/fraud resolution vendors
   – Printing, mailing and call center vendors
4. Develop relationship with relevant law enforcement agencies
5. Develop template security breach notifications and FAQs
6. Implement and test your security incident response plan
Security Incident Response Plan

1. Identify members of the security incident response team
2. Allocate roles and responsibilities
3. Establish a reporting mechanism for employees and business associates
4. Strategy for response, mitigation and remediation
5. Strategy for contacts with law enforcement
6. Strategy for handling the media
7. Documentation and preservation of evidence
8. Discipline for responsible employees
9. Post-incident review/“lessons learned”
10. Training
Is It A Breach?

- Is PHI involved? Is it “trigger data” under state law?
- Is the “trigger data” encrypted?
- Does an exception under HIPAA apply?

1. Unintentional, good faith acquisition, access, or use of PHI
   - **Example:** Nurse accidentally pulls a chart for the wrong patient
Is It A Breach?

2. Inadvertent disclosure of PHI by one authorized employee to another
   - **Example**: Doctor sends patient records to the wrong specialist

3. Disclosure of PHI to an unauthorized person who could not reasonably have retained it
   - **Example**: E-mail with PHI sent to the wrong employee’s corporate e-mail address but deleted before...
No breach under HIPAA if there is a “low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
2. The unauthorized person who used the PHI or to whom the disclosure was made
3. Whether the PHI was actually acquired or viewed
4. The extent to which the risk to the PHI has been mitigated

Other facts may be considered
Additional Considerations

- What is a “compromise”?
  - Not defined in the regulations
  - Probably means obtained, or potentially obtained, by an unauthorized third person who will misuse the PHI

- Burden is on the covered entity or business associate to establish a “low probability” of compromise

- Covered entity/business associate must document risk assessment

- Risk assessment **not** required if covered entity will provide notice
Know Your Deadlines

1. When was the breach discovered?
   - (a) Known, or by exercising reasonable diligence would have been known
   - (b) To any person, other than the person committing the breach
   - (c) Who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency)

2. Do you need law enforcement delay?

3. Beware of short reporting deadlines
   - CA: 5 business days to Dept. of Health Services
   - PR: 10 days to Dept. of Consumer of Affairs for breach of “data bank”
   - VT: 14 days to the state’s Attorney General
   - FL, OH, WI, VT: 45 days to individuals

4. Strive to complete notification within 30 days of discovery
Get Your Vendors Working

1. Involve breach counsel at the earliest possible stage
   - Establishes attorney-client privilege of communications with the SIRT and with breach response vendors

2. If your business associate discovered the breach, make sure it is handling the incident in accordance with the BAA

3. Get timelines and mailing list requirements from your notification vendor
   - Preparing the mailing list can be the most time consuming aspect of security incident response
   - Beware of special populations: minors, deceased, non-English speakers

4. Develop a press release if the breach could go viral
Prepare Your Notifications

Notice To Individual

- HIPAA’s content requirements are available at 45 C.F.R. pt. 164.404(c)
- Beware of outlier, state law requirements not preempted by HIPAA
- Get the tone right; assume the notice will be made public

Notice To HHS (and state agencies)

- HHS’ online notification form available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html
- Breach of fewer than 500 individuals, before March 1 of following year
- Breach of 500 or more individuals, when individuals are notified

Notice To The Media
After The Notices Go Out

- Have an FAQ ready to assist the contact person identified in the notice
- Have a strategy for handling returns
  - If 10 or more notices cannot be delivered, covered entity must prominently post the notice on its Web site for 90 days or in major media where affected individuals reside
- Determine whether any employees should be disciplined
- Conduct “lessons learned” session with SIRT
  - Modify existing safeguards or implement new ones
  - Provide additional training when appropriate
- Document the security incident response
Enhanced HIPAA Enforcement
Civil Penalty Enhancement

**Unknowing Violations:** $100 to $50,000 per violation

**Negligent Violations:** $1,000 to $50,000 per violation

- No penalty for unknowing and negligent violations corrected within 30 days of discovery

  - **Willful Neglect:** “Conscious intentional failure or reckless indifference to the obligation to comply”
    - $10,000 to $50,000 per violation (if corrected within 30 days)
    - $50,000 per violation (if not corrected)

- **$1.5M cap per calendar year for all violations of the same type**
HHS’ Enforcement Discretion

What is a violation?
HHS given broad discretion to identify individual violations for failure to comply

However, (a) each day of noncompliance counts as an additional violation, and (b) each individual harmed counts as a separate violation

– **Example**: Each day that a required safeguard is absent constitutes a separate violation

– **Example**: Each person whose PHI is compromised is a separate violation
HHS’ Enforcement Discretion

- Penalty can be imposed for underlying Privacy Rule violation even if the breach is properly handled

- Factors to be considered by HHS:
  1. The nature and extent of the violation
  2. Whether the violation caused financial, physical, reputational or other harm
  3. Covered entity’s history of compliance or non-compliance
  4. The financial condition of the covered entity
89,000 resolved complaints since April 2003, but nearly two-thirds were not investigated because:

(a) HHS lacked jurisdiction;
(b) The complaint was untimely or withdrawn;
(c) The complaint did not allege a violation

32,000 resolved complaints:

(a) 69% have resulted in corrective action
(b) 31% in a finding of no violation

Criminal Referrals to DOJ: 95,000 total complaints received have result in only 526 criminal referrals, i.e., less than 1%.
Most Common Complaints

1. Impermissible uses and disclosures of PHI
2. Lack of safeguards for PHI
3. Lack of patient access to PHI
4. Uses or disclosures of more than the minimum necessary PHI
5. Lack of administrative safeguards for electronic PHI

(HHS Enforcement Summary as of 3/31/14)
Most Common Targets of Complaints

1. Private Practices
2. General Hospitals
3. Outpatient Facilities
4. Health Plans (group health plans and health insurance issuers)
5. Pharmacies

(HHS Enforcement Summary as of 3/31/14)
HHS Enforcement Tactics

- HHS will use security breach notification as a means for identifying targets
  - 11 of 16 monetary settlements since 2011 triggered by breach report to HHS
  - Trigger breach can involve fewer than 500 individuals

- HHS tracks media reports
  - CE disclosed PHI to the media; TV news report of breach

- HHS will investigate far beyond the cause of the breach
  - County’s initial report of breach resulted in finding of widespread violations

- If PHI was publicly accessible, burden is on covered entity to show the information was not accessed
Since early 2011, HHS has been obtaining significant monetary settlements:

- 16 publicly announced settlements since January 2011
- 1 settlement exceeded $4M
- Average settlement = $1M
9 of 16 incidents involved acts by employees

1. $1.5M settlement with Mass Eye & Ear after theft of laptop containing unencrypted PHI of 3,621 patients

2. $1.7M settlement with Alaska DHHS after theft from employee’s vehicle of USB hard drive possibly containing PHI

3. $1M settlement with Mass General after employee left 192 HIV patients records on subway

4. $865,000 settlement with UCLA Medical Center after hospital employees allegedly accessed the records of two celebrity patients without authority

5. $275K settlement after executives at Shasta Regional Medical Center disclosed a patient’s PHI to the media
Common Compliance Shortfalls

1. Failure to conduct a risk assessment and risk management process
2. Lack of adequate policies and procedures
3. Failure to implement a security incident response plan
4. Failure to provide security breach notification when required
Common Compliance Shortfalls

5. Failure to address mobile device security
6. Lack of, or inadequate, training
7. Failure to discipline workforce members responsible for violation
8. Lack of adequate security controls
State attorneys general can sue in federal district court to recover damages to state residents caused by a HIPAA violation

- **01/13**: Mass AG obtains $140K consent judgment from a medical billing company and seven physicians who contracted with it based on alleged improper disposal of PHI.

- **07/11**: Indiana AG announces that major provider agreed to pay $100K to settle charges that the company had unreasonably delayed security breach notification.

- **07/10**: CT AG announces settlement with insurer over its loss of a computer disk drive containing the PHI of $1.5M individuals nationwide.
Steps To Reducing Enforcement Risk?

1. Implement all required policies and procedures and update them periodically to reflect material changes.

2. Conduct a risk assessment and promptly address all critical risks.
   - 4/122/14: Concentra settled breach-induced investigation for $1.7 million where cause of breach was an unaddressed risk.

3. Encrypt all portable devices containing PHI.

4. Train employees periodically on HIPAA compliance and send periodic information security reminders.

5. Prepare for a security breach; “it happens to the best of us.”
Contact Information

Philip L. Gordon, Esq.
Littler Mendelson, P.C.
303.362.2858
pgordon@littler.com
Visit Littler’s Practice Group blog:
www.workplaceprivacycounsel.com