What Does The New Omnibus HIPAA/HITECH Final Rule Really Mean For Employers And Their Service Providers?

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

Russell Chapman, Esq.
Littler Mendelson, P.C.
214.880.8177
RChapman@littler.com
presented by:

Philip L. Gordon, Esq.
PGordon@littler.com
303.362.2858
Denver Office

Russell Chapman, Esq.
RChapman@littler.com
214.880.8177
Dallas Office
TODAY’S AGENDA

I. HIPAA Overview
II. Overview Of Omnibus Final Rule
III. HIPAA Security Breach Notification
IV. Enhanced HIPAA Enforcement
V. What Should Your Organization Be Doing
VI. Business Associates & Business Associate Agreements
VII. GINA, HIPAA And Privacy Notices
VIII. Other Changes To HIPAA
HIPAA Overview
HIPAA Regulations

- HIPAA Transaction Rule
  - Requires the use of electronic codes for administrative functions related to healthcare, including:

<table>
<thead>
<tr>
<th>Healthcare claims</th>
<th>Plan eligibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare payment</td>
<td>Health plan premium payments</td>
</tr>
<tr>
<td>Coordination of benefits</td>
<td>Referral certification</td>
</tr>
<tr>
<td>Health care claims status</td>
<td>Health claims attachments</td>
</tr>
<tr>
<td>Enrollment &amp; disenrollment</td>
<td>First report of injury</td>
</tr>
</tbody>
</table>
HIPAA Regulations

The HIPAA Privacy Rule
  – Privacy protections for health information

The HIPAA Security Rule
  – Technical safeguards for electronic health information

HITECH Act & Interim Regulations
  – Security breach notification
  – Enhanced enforcement
  – New requirements for business associates
What Health Plans Are Covered?

- Group health, vision and dental plans
- Pharmacy benefit plans
- Health care reimbursement flexible spending accounts
- Employee assistance programs
- Long-term care plans
“Health Plan” Excludes:

- Disability Income Insurance
- Stop-gap Insurance Coverage
- Workers’ Compensation Insurance
- Most Health Savings Accounts (HSA’s)
- Automobile Liability Insurance
- Coverage For On-Site Medical Clinics
What Information Is Covered?

Protected Health Information ("PHI")

- Information created or received by a health plan or covered healthcare provider; and
- Relates to the condition or care of an individual; or
- Relates to the payment for care; and
- Permits identification of the individual

- Includes demographic and identification information
What Information Is Covered?

- Enrollment And Disenrollment
- Utilization Reports
- Claims Administration
- Explanation Of Benefits
- Claims Adjudication
- Health FSA Contributions And Usage
What Information Is Excluded?

- Employee Personnel Records Are Excluded
  - Sick leave requests
  - FMLA certifications
  - ADA-related information
  - Employee gossip
  - Drug test results
Who Is a Business Associate?

- Business associates = those who use PHI to perform, or assist the covered entity to perform, its covered functions

- Business associate services
  - Insurance Broker
  - Lawyer, Accountant, Auditor
  - Third-Party Administrator
  - Pharmacy Benefits Manager
  - Large Case Manager
  - Disposal Company
Key Compliance Obligations

1. Restrict access to PHI to employees who perform plan administration functions

2. Use and disclose PHI only as permitted under the HIPAA Privacy Rule

3. Implement safeguards in the HIPAA Security Rule for electronic PHI

4. Notify plan participants of any security breach
5. Enter business associate agreements with business associates

6. Notify employees of the plans’ privacy practices

7. Establish policies and procedures to administer plan participants’ HIPAA rights

8. Amend plan documents
The HIPAA/HITECH Omnibus Final Rule
What Has Not Changed

Fundamental compliance obligations for HIPAA-covered plans remain unchanged
What Is New?

1. Threshold for security breaches has been lowered
2. Enforcement risk has increased
3. Business associates and subcontractors subject to direct regulation
4. Business associate agreements need to be amended
5. Privacy notices need to be revised and redistributed
6. Increased risk of GINA enforcement
7. Other changes: (a) right to electronic copies of PHI, (b) restrictions on disclosure of PHI to the plan
What Are The Key Deadlines?

Omnibus Final Rule:

01/25/13: Published in Federal Register

03/26/13: Effective (Enforcement Rule)

09/23/13: Compliance deadline for most changes

2013 Open Enrollment: Revised privacy notices

09/22/14: Final deadline for BAAs
HIPAA Security Breach Notification
Trigger Event

- Notification must be provided when there is a “breach” of “unsecured PHI”
PHI is “unsecured” unless:

- It is encrypted
  - Encryption = an algorithmic process has been applied to create “a low probability of assigning meaning without the use of a confidential process or key” and the key has not been breached
  - See NIST Special Publications 800-11, 800-52, 800-77, and 800-113

- It has been rendered irretrievable
  - Paper: Shredded
  - Electronic: Purged (NIST Special Publication 800-88)
New Definition Of “Breach”

- **Until 9/23/13:** “Breach” = unauthorized access to, or acquisition, use, or disclosure of, PHI that poses a significant risk of financial, reputational or other harm.

- **After 9/23/13:** “Breach” = any unauthorized access to, or acquisition, use, or disclosure of, PHI subject to four exceptions.
Three Existing Exceptions

1. Unintentional, good faith acquisition, access, or use of PHI

   Example: Benefits manager accidentally reviews benefits information for an employee not assigned to the benefits manager

2. Inadvertent disclosure of PHI by one authorized employee to another

   Example: Benefits manager for one business unit intending to send PHI to the plan participant accidentally sends it to the benefits manager for another business unit

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 opened
New Exception

No breach 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 might 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
Examples Of Common Security Incidents

1. E-mail attachments containing PHI that are sent to the wrong recipient or to the correct recipient but containing someone else’s PHI
2. The loss or theft of a portable electronic storage device containing PHI
3. EOBs sent to the wrong plan participant
4. EOBs with PHI either printed on the envelope or viewable through a clear envelope window
5. Benefits web sites that because of a technical error permit viewing of one plan participant’s PHI by other plan participants
Notice by Business Associate to Covered Entity

1. Notice must be provided “without unreasonable delay” and no later than 60 days after discovery

2. Notice must include:
   - An identification of each affected individual
   - Any information that the covered entity is required to include in its notice to affected individuals
1. First day that the incident is known to a member of the covered entity’s or business associate’s workforce (other than the responsible individual)

2. First day that the covered entity or business associate would have known of the incident “by exercising reasonable diligence”
   - “Reasonable diligence” means “business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances”
Covered Entity’s Obligations

1. Notify affected individuals within 60 days of discovering the breach

2. Notify HHS contemporaneously with notice to individuals if the breach involves more than 500 individuals; otherwise, notify HHS by March 1 of following calendar year

3. Notify prominent media outlets if the breach involves more than 500 individuals in a specific geographic location
Enhanced HIPAA Enforcement
All publicly announced settlements in 2011 and 2012 arose from security breaches

1. $50,000 settlement with Hospice of Northern Idaho after theft of laptop containing unencrypted PHI of 441 patients
2. $1.5M settlement with Mass Eye & Ear after theft of laptop containing unencrypted PHI of 3,621 patients
3. $1.7M settlement with Alaska DHHS after theft from employee’s vehicle of USB hard drive possibly containing PHI
4. $100,000 settlement with Phoenix Cardiac Surgery which posted clinical and surgical appointments in Internet-based calendar that was publicly available
Breach-Driven Enforcement

5. $1.5M settlement with BCBS of TN over the loss of 57 hard drives containing 1M patient records

6. $865,000 settlement with UCLA Medical Center after hospital employees allegedly accessed the records of two celebrity patients without authority

7. $1M settlement with Mass General after employee left 192 HIV patients records on subway
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.
Responsibility For Business Associates

Covered entity can be held responsible for business associate’s HIPAA violations

**Key:** Is the business associate acting as an agent as defined by federal common law?
Responsibility For Business Associates

“The right or authority to control the business associate’s conduct . . . is the essential factor in determining whether an agency relationship exist.”

- BAA grants the covered entity the authority to direct the performance of the service provided by its business associate

- **Example:** BAA states, “business associate must make available protected health information in accordance with§164.524 based on the instructions to be provided by or under the direction of a covered entity”
Responsibility For Business Associates

Virtually no relevant case law applying the federal common law of agency to contracting entities

- What can be gleaned from the case law?
  - Degree of control over the conduct and activities of the putative agent’s acts is critical
  - An agency relationship can be implied from the facts notwithstanding contract language to the contrary
  - Principal is not liable for acts of the agent outside the scope of the agency

  - Example: Agent acts on its own behalf
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

Key Point: HHS no longer is required to seek voluntary resolution of unknowing and negligent violations
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 physical, financial, reputational or other harm
3. Covered entity’s history of compliance or non-compliance
4. The financial condition of the covered entity
What Should Your Organization Be Doing?
Access Controls

- Only employees who perform plan administration functions have authorized access
- Authorized employees should be known to be trustworthy
- Modify access rights when job duties change
- Terminate access promptly upon termination of employment
Portable Devices

- Establish rules for saving PHI to laptops, thumb drives, CDs, and other portable media

Examples:

1. Encrypt all portable devices used to store PHI
2. Limited to only certain categories of employees
3. Limited to only certain purposes
4. PHI must be deleted after purpose is accomplished
1. Stored in locked drawers, desks or offices when unattended
2. Clean desk policy
3. Don’t remove from office unless absolutely necessary
4. Open your own mail if you receive PHI by mail
5. Promptly remove paper documents containing PHI from printers, fax machines and copiers
6. Confirm recipient’s fax number before transmitting PHI
Protections For Oral PHI

- Prevent overhearing of office conferences and telephone calls involving PHI
- Do not leave voicemail containing PHI in general voice mail boxes or when you know others might overhear the recording
Proper Disposal Of PHI

- Consult with IT department before discarding any computer or storage device (e.g., thumb drive, CD) that contains PHI

- Shred paper documents containing PHI before discarding
Physical Safeguards

1. Prevent unauthorized access to facilities and workstations

2. Control authorized access to facilities and workstations

3. Track the movement of hardware and electronic media and create a duplicate of PHI, when necessary, before movement
Security Awareness Training

- Roles of employees in adhering to, and enforcing, security policies
  - Procedure for guarding against and reporting malicious software
  - Log-ins will be monitored
  - Password management
    - Guidelines for creating, changing and safeguarding passwords
Incident Response Planning

1. Build an incident response team
2. Define roles and responsibilities
3. Ensure “24/7” availability of team members
4. Establish protocols for reasonably foreseeable incidents
5. Establish reporting procedure for employees and business associates
Reduce Risk Of Common Security Breaches

1. Prohibit storage of PHI on portable devices or implement encryption
2. Encrypt e-mail containing PHI where feasible
3. Additional training/periodic reminders to prevent mis-addressed e-mail and incorrect attachments
4. Clearance procedures for mass e-mails and paper mailings containing PHI
5. Implement data loss prevent (DLP) software
6. Carefully vet security procedures of vendors mailing EOBs
Security Incident Response

1. Plan for mis-directed e-mails: recalls, mass deletions, phone calls

2. Make efforts to recover lost or stolen laptops and conduct forensics

3. Promptly patch security holes in benefits websites

4. Plan to correct discovered violations within 30 days of discovery
New Rules For Business Associates And Business Associate Agreements
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 compilation of an individual’s health records drawn from multiple sources and managed, shared and controlled by the individual

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

   **Example**: E-prescribing gateways
1. **Business associates now have a direct statutory obligation to comply with:**
   - The HIPAA Security Rule
   - The privacy–related obligations in business associate agreements:  (a) use and disclose PHI only as permitted by BAA or the Privacy Rule; (b) use, disclose and request minimum necessary PHI; (c) respond to individual requests to exercise HIPAA rights

2. **Business associates are directly subject to criminal and civil liability for violations**

3. **Business associates are directly subject to audit by HHS**
Downstream Contracting

1. First-tier business associates must enter into business associate agreements with subcontractors

2. Subcontractors must agree to enter into business associate agreements with their subcontractors

3. Subcontractors can use PHI only for the same purposes, or a subset of purposes, for which the BA may use PHI, but not any new purposes

4. BA’s are liable for penalties resulting from acts or omission of subcontractors who are agents

- **Covered entities are not required to have any contractual relationship with subcontractors or to list subcontractors in the business associate agreement**
Mandatory Revisions To BAAs

Business associate agreements must now 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
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
Optional Revisions To BAAs

1. Language suggesting agency relationship
   ➢ **Note**: BA can be both an agent and a contractor

2. List specific information security safeguards

3. Timing and content of notice of incident

4. Determination whether incident is a breach

5. Control over notification process

6. Reimbursement of incident response costs
Optional Revisions To BAAs

7. Audits of information security practices
8. Indemnification and cyber-risk insurance
9. Inapplicability of loss limitations
10. Prohibition on sale of PHI
11. Prohibition on use of PHI for underwriting
HHS has updated the sample agreement at its website

URL:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
BAA-Related Deadlines

- Existing BAAs are compliant through 9/22/14
- If BAA is revised after the effective date of 3/26/13, the required language must be included in the revised agreement
- Business associates must enter BAAs with subcontractors by 9/23/13
GINA, HIPAA And Privacy Notices
GINA Incorporated Into HIPAA

- PHI includes genetic information as defined by GINA
  - “Genetic information” includes family medical history

- HIPAA prohibits the use of PHI that is genetic information for underwriting purposes
  - “Underwriting purposes” includes the offering of incentives, such as rebates or discounts, to complete a health risk assessment (HRA)

- Violation of the restriction on HRAs opens employers to HIPAA’s much richer penalty scheme
The Bifurcated HRA

- Offer financial inducement for employees to respond to questions that do not call for genetic information
  - **Note**: Need to consider limitations on inducements

- Clearly & conspicuously (a) identify questions calling for genetic information, and (b) inform employees that they can earn the financial inducement even if they do not answer those questions
Disease Management

- If genetic information provided in response to the HRA reveals a heightened risk of disease, the employer can offer a financial inducement to participate in a voluntary wellness program.

- To avoid unlawful discrimination, employees with current health conditions and unhealthy life styles must be permitted to participate equally.
Privacy notices must now include the following statements:

1. Health plans are required to obtain plan participants’ authorization to
   a. use or disclose psychotherapy notes (where applicable)
   b. use PHI for marketing purposes or to sell PHI
   c. use or disclose PHI for any purpose not described in the notice

2. The plans (other than a long-term care plan) are prohibited from using PHI that is genetic information for underwriting purposes

3. Plan participants have the right to receive notice when there is a breach of their unsecured PHI
Employers with benefits sites: (a) post the revised notice by 9/23/13; and (b) distribute notice in next annual mailing to plan participants

Employers without benefits sites: (a) revise the notice effective 9/23/13, and (b) distribute the notice by 11/22/13

Distribution by e-mail: Is permitted as long as the named insured agrees to electronic delivery
Other Changes To HIPAA
Right To Access ePHI

Right to receive PHI in electronic form

- Must respond within 30 days regardless of location of PHI
- Not required to scan paper documents
- Applies to all electronic PHI used to make benefits decisions
- Production may be by unencrypted e-mail if accompanied by a warning
- Must follow instructions to send to third party
Right To Pay In Cash

- Plan participants have the right to pay a provider in cash and instruct the provider not to send to the plan any PHI related to the paid services.
1. Update security incident response plan to reflect new breach standard
2. Create form to document risk assessment
3. Review, and if necessary, update safeguard policies
4. Update template BAA
5. Update and redistribute Notice of Privacy Practices
6. Revise procedures to address requests for access to ePHI
THANK YOU

Visit our Practice Group blog: www.workplaceprivacycounsel.com

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

Russell Chapman, Esq.
Littler Mendelson, P.C.
214.880.8177
RChapman@littler.com