HIPAA Enforcement 2.0: Minimizing Exposure with Affirmative Defense

FairWarning® Ready Executive Webinar Series
June 4, 2013
• HIPAA Omnibus Rule’s effects on future enforcement
• Take advantage of overlooked additions to the rule which will *help your organization in case of a breach*
• Minimize or eliminate your exposure to civil monetary penalties (CMPs)
• Avoid situations likely to trigger an audit
• The case for compliance investment
• Positioning for affirmative defense
HIPAA Enforcement 2.0: Minimizing Exposure

EDWARD F. SHAY
POST & SCHELL, PC
Agenda

- Pre-HITECH Enforcement
- How the HITECH Act Changed Enforcement
- Enforcement added by the Final HITECH Rule?
- New Enforcement exposures for CEs and BAs
- Corrective Action Affirmative Defense
  - What is affirmative defense
  - How affirmative defense works
- Readiness and the duty to monitor
Terminology

- Agents
- Civil Monetary Penalties (CMPs)
- Culpability
- Actual vs. Constructive Knowledge
- Interim Final Enforcement Rule
- Reasonable Diligence
- Violation
HIPAA Enforcement
Before HITECH

• Old HIPAA—single violation $100/$25,000 per year—unless could not have known

• Violators only “covered entity”

• Criminal penalties only for “covered entity”

• Complaint driven enforcement
HITECH Act and Enforcement

- HITECH Act greatly expanded enforcement
  - Extended violations to business associates
  - Extended criminal sanctions to any “individual without authorization”
  - CMPs for much larger amounts
  - State AG enforcement—up to $25,000 penalties—with attorneys fees
  - Only affirmative defense is corrective action
  - OCR must investigate of willful neglect
A Sample of Post-HITECH Enforcement Cases

- Mass Eye and Ear Infirmary, breach of ePHI, inadequate analysis of risks, could not/did not monitor user access, $1.5M, 9/13/2012
- Hospice of Northern Idaho, breach, theft of laptop affecting 441 individuals, inadequate analysis of risks, $50,000, 12/28/2012
- Idaho State University, inadequate analysis of risks, failure to monitor system activity, $400,000, 5/10/2013
Key Changes to the Enforcement Rule

- Six major impacts to the Enforcement Rule
  - Penalty amounts/ranges were adopted from the Interim Final Rule
  - Culpability removes affirmative defense for state of mind
  - Business Associates and Subs subject to Enforcement Rule
  - Covered Entities and Business Associates liable for their “agents”
  - OCR will investigate all possible violations due to willful neglect
  - Mitigation an affirmative defense
Penalty ranges were adopted from the Interim Final Rule.

<table>
<thead>
<tr>
<th>Culpability</th>
<th>Amount per single violation</th>
<th>Cal. year same violation max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Corrected</td>
<td>$10,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Not corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Culpability Removes Affirmative Defense for State of Mind

<table>
<thead>
<tr>
<th>Culpability</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know-Could Not Know</td>
<td>Strict liability</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>Knew, would have know but beyond control</td>
</tr>
<tr>
<td>Willful Neglect-Corrected</td>
<td>Intentional failure, reckless indifference</td>
</tr>
<tr>
<td>Willful Neglect-Not Corrected</td>
<td>Intentional failure, reckless indifference</td>
</tr>
</tbody>
</table>
Could Not Know/Should Have Known and Reasonable Diligence

- Except for “willful neglect” tiers, must show “reasonable diligence”
- Reasonable diligence requires “business care and prudence” of one seeking to comply
- Differentiates two lower tiers from willful neglect tiers
Business Associates and Subs Subject to Enforcement Rule

- New 160.300 that “this subpart applies to actions by the Secretary, covered entities, business associates and other...” 78 Fed. Reg. 5690, (January 19, 2013)
- No way for Business Associate to limit effect of rule to a health care component. All or nothing effect greatly increases cost of compliance
Covered Entities and Business Associates Liable for Their Agents

- Return of ascending liability
- Violations by the agents will be attributed to its principal covered entity or business associate
- Test is federal common law of agency—facts and circumstances indicating control
- If only recourse for covered entity is to amend or sue for breach—then likely an independent contractor
Covered Entities and Business Associates Liable for Their Agents

- Why does it matter? Constructive knowledge
- The breach notification rules suggested that a covered entity could have both “agent” business associates and “independent contractor” business associates
- Discovery by “agent” BA attributed same as workforce. Duty to train “agents”
OCR Will Investigate all Possible Violations Due to Willful Neglect

- OCR revised § 160.312 so that the Secretary may move directly to a civil money penalty without exhausting informal resolution efforts at her discretion, particularly in cases involving willful neglect violations
- OCR screens every complaint that it receives
- OCR will investigate any complaint that alleges “possible” willful neglect
The Corrective Action Affirmative Defense

- Applies to all HIPAA violations (Privacy, Security, Breach and Standard Transactions)
- Violations occurring after 2/18/2009
- Violations by Covered Entities or Business Associates
- Corrected within 30 days after actual or constructive knowledge from “reasonable diligence” or
- Willful neglect--but timely corrected
Purpose of Corrective Action
Affirmative Defense

Department of Health & Human Services wishes to encourage “establishment of a compliance program that:

• Proactively prevents,
• Detects,
• And corrects indications of noncompliance”

Actual vs. Constructive Knowledge

• Actual:
  - Knew, via complaint, internal processes, notification by employee/BA, or notification by Health & Human Services

• Constructive:
  - Should have known
  - Other sources of information exist that establish knowledge
  - Specifically unusual access or audit log activity
Is Corrective Action Already a HIPAA Obligation?

- Security Rule standard for Security management and duty to “correct security violations.”
- Privacy Rule standards on sanctions for “failure to comply” and mitigation of “any harmful effect”
- Breach Notification notice of steps being taken to mitigate harm and avoid further breaches
Essential Elements for establishing Affirmative Defense

- Reasonable diligence - duty to monitor
  - Periodic risk assessments
  - Complaints
  - On-going auditing of system activity
  - Security Incidents
- Capabilities - a rapid response team
  - Resources - budget, insurance
  - Policies
  - Re-training
Observations

• OCR holds all the face cards
• Cannot win in a dispute with OCR
• Can maximize circumstances using the 30 day corrective action affirmative defense
• Focus on monitoring and quickly responding to possible violations
• Dollars spent on prevention and monitoring better than dollars spent on OCR
Questions or Comments?

Edward F. Shay
eshay@postschell.com
Responding to Privacy Breaches: The Full Cost

FairWarning® Ready Executive Webinar Series
June 4, 2013
The Case for Compliance Investment

Available after today’s webinar:

- Breach Damages Estimator
  - Comprehensive and variable based estimation of financial damages resulting from incident which is reported to the media
  - Based on privacy monitoring deployments as well as interviews with health systems, legal counsel and 3rd-parties involved with high-profile breaches and audits
  - No-charge FairWarning® open copyright license

Email Solutions@Fairwarning.com
Positioning for Affirmative Defense

• Proactively detect potential breaches
• Have a plan to discover, investigate and manage incidents in a timely manner
• Be actively mitigating identified breaches (both for Affirmative Defense and to head off larger issues)
FairWarning® & HIPAA Omnibus

• Increased volume of reportable breaches
• Need for automation
• Need for incident tracking & reporting
Next Steps

- See a demo of FairWarning® 3.1.5
- Request the Breach Damages Estimator by emailing Solutions@FairWarning.com
- Questions?
Contact Information

Edward F. Shay
Principal, Post & Schell, P.C.
eshay@postschell.com

Shane Whitlatch
Executive Vice President
FairWarning®
Shane@FairWarning.com