Breach Notification: Who, when, what, and how?

Jill Moore, UNC School of Government
September 2017

Review: What is a breach?

- Acquisition, access, use, or disclosure of protected health information (PHI) that:
  - Is not authorized by the HIPAA privacy rule, and
  - Compromises the privacy and security of the PHI.

- Breach is *presumed* unless:
  - A specific exception in the rule applies, or
  - A risk assessment shows a low probability that PHI was compromised.
Was it encrypted or disposed per rules (safe harbor)?

Did acquisition, access, use, or disclosure involve PHI?

Low probability of compromise per risk assessment?

STOP

Did acquisition, access, use, or disclosure involve PHI?

Notification required

STOP

Does an exception apply?

Exceptions

- PHI could not reasonably be retained
- Access is unintentional and by a workforce member or business associate acting in good faith
- Inadvertent disclosure is made to another person within the CE or BA who is authorized to access PHI
Risk Assessment

What it is:
- Analysis you undertake to demonstrate low probability that PHI was compromised
- Demonstrated low probability of compromise defeats the presumption that unauthorized acquisition, access, use, or disclosure was a breach

Minimum factors:
- Nature and extent of PHI, including types of identifiers & likelihood of re-identification
- Unauthorized person who received disclosure or used PHI
- Whether PHI was actually acquired and viewed
- Extent to which any risk to PHI has been mitigated

Notification prep: date check

- If required to notify, must do so “without unreasonable delay” – no later than 60 days after breach discovered
- Breach deemed discovered even if no actual knowledge, if reasonable diligence would have revealed it
Notification Timeframes

**Individuals**
- Without unreasonable delay, no later than 60 days after breach discovered

**US DHHS Secretary**
- > 500 individuals: contemporaneous w/individual notice
- < 500 individuals: no later than 60 days after the end of the calendar year when the breach is discovered

**Media (only if more than 500)**
- Without unreasonable delay, no later than 60 days after breach discovered

Notifying individuals

**When is notification required?**
- Whenever there is a breach involving one or more individual

**How do you do it?**
- Letter sent by first-class mail
- Can use email instead *only if* CE has previously obtained the individual's agreement to be notified of breaches by email
- If situation requires urgency because of possible imminent misuse of PHI, may notify by telephone or other means, but still send letter
Notifying individuals

What if the CE’s contact information for a person is insufficient or out of date?

- Substitute notice is allowed
- < 10 individuals in this situation, may use other form of written notice, telephone, or other means
- > 10 individuals, must either:
  - Post notice on home page of website for 90 days, or
  - Provide notice in major print or broadcast media where affected individuals likely arise

Notifying individuals

What must the notice include?

- Description of incident, including dates of breach and of discovery
- Description of types of PHI involved (e.g., name, address, record number, DOB, diagnosis, etc.)
- Any steps individual(s) should take to minimize potential harm from the breach
- Brief description of CE actions to investigate and mitigate the breach, and protect against future breaches
- Contact procedures for individuals to ask questions or learn more about breach
Notifying DHHS

When is notification required?

- Only when there’s a breach of unsecured PHI requiring notification.
- Number of individuals affected determines timing of notification:
  - 500 or more: same time as individual notification
  - Less than 500: within 60 days of end of calendar year

How do you do it?

- Online through HHS website
- One report per breach
What must the notice to DHHS include?

<table>
<thead>
<tr>
<th>General &amp; Contact Info</th>
<th>Breach info</th>
<th>CE actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Report type</td>
<td>• # of individuals</td>
<td>• Date notice provided</td>
</tr>
<tr>
<td>• Entity and contact info</td>
<td>• Dates (breach &amp; discovery)</td>
<td>• Was substitute notice required</td>
</tr>
<tr>
<td>• Business associate info, if applicable</td>
<td>• Type: hacking/IT, improper disposal, loss, theft, unauthorized access/disclosure</td>
<td>• Was media notice required</td>
</tr>
<tr>
<td></td>
<td>• Location: laptop, paper, mobile, etc.</td>
<td>• Actions taken in response to breach: long checklist including technological and policy changes, employee sanctions, re-training of workforce or BAs, help provided to individuals affected, and more</td>
</tr>
<tr>
<td></td>
<td>• Type of PHI: clinical, demographic, financial, other</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Description (open-ended)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Safeguards in place</td>
<td></td>
</tr>
</tbody>
</table>

Notifying the media

When is notification required?
• Only when there’s a breach involving 500 or more people

How do you do it?
• Press release to appropriate media outlets serving the affected area

What should the notice include?
• Same information as the letter to individuals
Breach resources

• HIPAA regulations: 45 CFR 164, subpart D (sections 164.400 – 164.414)

• US DHHS resources:
  http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html