HIPAA “Safe Harbor” Requirement

Encryption

Lessons Learned

From the Real World

Larry.Yob@AscensionHealth.org
Scott.Aschenbach@StJohn.org
Breach

45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information

• Section 13400(1) of the Act defines
  – “breach” to mean, generally, the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information
Exemptions from Breach Notification Requirements

• Limited Data Set - A limited data set must have all direct identifiers removed from the protected health information (name, address, social security number, and account number of an individual or the individual’s relative, employer, or household member).
Exemptions from Breach Notification Requirements

• Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

• Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:
  – Destroyed
  – Encrypted
Exemptions from Breach Notification Requirements - Destroyed

• The media on which the PHI is stored or recorded have been destroyed in one of the following ways:

  – (i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

  – (ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.
Exemptions from Breach Notification Requirements – Encrypted

• Electronic PHI has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” and such confidential process or key that might enable decryption has not been breached.

• Valid encryption processes for data at rest are consistent with NIST Special Publication 800–111, Guide to Storage Encryption Technologies for End User Devices.
Exemptions from Breach Notification Requirements – Encrypted

• Full Disk Encryption - pre-boot authentication is required
• Virtual Disk Encryption and Volume Encryption
• File/Folder Encryption
Procedure for Lost Mobile Devices

<table>
<thead>
<tr>
<th>Other Device</th>
<th>Android</th>
<th>iOS (Apple)</th>
<th>Laptop/tablet</th>
<th>BlackBerry</th>
</tr>
</thead>
<tbody>
<tr>
<td>No ActiveSync</td>
<td>No ActiveSync</td>
<td>No ActiveSync</td>
<td>No encryption</td>
<td>Not Secure</td>
</tr>
<tr>
<td>ActiveSync Default Policy Settings Applied</td>
<td>ActiveSync or Security App Secure</td>
<td>Full Disk or Partial Encryption</td>
<td>Blackberry Secure</td>
<td></td>
</tr>
<tr>
<td>ActiveSync Secure Policy Settings Applied</td>
<td></td>
<td>Full Disk with Pre-Boot Authentication</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assess Risk:
- Password set?
- Auto-lock set?
- Data on removable SD card?
- ePHI via email?
- ePHI files stored locally?
- Other EMR applications used?
- Direct identifiers, DOB, zip?
- Reported & wiped quickly?
- Device used since loss?
- Device reporting in at all?

Risk of Significant Harm?
- Yes
- No

No Risk of Significant Harm
- No Action Required

Risk of Significant Harm
- Over 500?
- Yes
- No
- Yes

- Notify Individuals w/in 60 days
- Notify OCR next March

- Notify “prominent media outlets” and OCR w/in 60 days

“Safe Harbor” No Action Required
### Step 1: Determine Type/Status of Lost Mobile Device

<table>
<thead>
<tr>
<th></th>
<th>Other Device</th>
<th>Android</th>
<th>iOS (Apple)</th>
<th>Laptop/tablet</th>
<th>BlackBerry</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveSync</td>
<td>No ActiveSync</td>
<td>No ActiveSync</td>
<td>No ActiveSync</td>
<td>No encryption</td>
<td>Not Secure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Full Disk or Partial Encryption</td>
<td>Secure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Full Disk with Pre-Boot Authentication</td>
<td>Secure</td>
</tr>
</tbody>
</table>

Was the device adequately protected by encryption?

- **A** ➔ Encryption working unless it’s properly enabled.
- **B** ➔ iOS & Blackberry encrypt data at rest, but this is useless unless a non-trivial password & auto-lockout were provably set on the device.
- **C** ➔ Even w/ the most secure ActiveSync settings, the loss of some devices will still have to be reported.
- **C** ➔ Security software can adequately protect almost any “smart” device, and can be more convenient to users.
### Step 2: Is Information on the Device Indecipherable?

<table>
<thead>
<tr>
<th>Device Type</th>
<th>OS</th>
<th>ActiveSync</th>
<th>Security Policy</th>
<th>Encryption Type</th>
<th>Security State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other Device</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Full Disk or Partial</td>
<td>Not Secure</td>
</tr>
<tr>
<td></td>
<td>ActiveSync</td>
<td>ActiveSync</td>
<td>Default Policy</td>
<td>Encryption</td>
<td>Secure</td>
</tr>
<tr>
<td>iOS (Apple)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Full Disk with Pre-Boot</td>
<td>BlackBerry Secure</td>
</tr>
<tr>
<td>Android</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Encryption</td>
<td>Secure</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>Not</td>
<td>No</td>
<td>No</td>
<td>Encryption</td>
<td>Secure</td>
</tr>
<tr>
<td>Laptop/tablet</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Full Disk</td>
<td>Not Secure</td>
</tr>
<tr>
<td></td>
<td>ActiveSync</td>
<td>ActiveSync</td>
<td>Default Policy</td>
<td>Encryption</td>
<td>Secure</td>
</tr>
<tr>
<td></td>
<td>or Security App</td>
<td>Secure</td>
<td>Settings Applied</td>
<td></td>
<td>BlackBerry Secure</td>
</tr>
</tbody>
</table>

**“Safe Harbor”**
No Action Required

**Be sure to involve**
- Management
- Legal
- Corporate Responsibility

**If you can prove the lost device is in the green area:**
- There is no requirement to report the loss
- The information is considered indecipherable.
Step 3a: Assess Risk if Data is Potentially Decipherable

You’ll need to consider all these factors when deciding whether an unauthorized person now has access to protected information.

A: Device Protection

• Remote-wiped device before it could be used by a thief?
• Data on SD card that can be read outside device OS controls?

Assess Risk:

• Password set?
• Auto-lock set?
• Data on removable SD card?
• ePHI via email?
• ePHI files stored locally?
• Other EMR applications used?
• Direct identifiers, DOB, zip?
• Reported & wiped quickly?
• Device used since loss?
• Device reporting in at all?

• Auto-lock set so device requires password when used?
• Non-trivial password, or
• Short passcode w/ limited # of attempts?
• Found by another authorized person? (not really a breach then)
Step 3b: Assess Risk if Data is Potentially Decipherable

B: What Data Was On The Device?
- Examine your e-mail history – what was sent?
- How long was e-mail configured to be cached on the device?
- Were attachments with protected data saved locally to device memory?
- Were clinical or corporate applications used on the device that store information locally?

Assess Risk:
- Password set?
- Auto-lock set?
- Data on removable SD card?
- ePHI via email?
- ePHI files stored locally?
- Other EMR applications used?
- Direct identifiers, DOB, zip?
- Reported & wiped quickly?
- Device used since loss?
- Device reporting in at all?

- What other ways could protected data be captured locally?
  - SMS/text
  - Non-corporate e-mail accounts
  - Web downloads
  - Camera, device screen snapshots
  - Other applications, sanctioned or not
Step 4: Assess Risk of Significant Harm

Can the information disclosed cause “significant risk of financial, reputational, or other harm to the individual”?

- **Financial Harm**
  - SSN, DOB or other information that could be used to steal an identity or falsely identify themselves

- **Reputational Harm**
  - Not just that they’ve had hospital services
  - Diagnosis, procedures, codes, that harm their reputation
  - Locations, comments, pictures indicating such a diagnosis

Risk Analysis tools available (more links in the notes)

- Flow chart: [www.hipaacow.org](http://www.hipaacow.org) (Wisconsin)
- AHIMA (American Health Information Management Assoc.)
Step 5: Notification

You’ll work with others in your organization, but duties you may be called upon to perform:

• Scan all breached data to find comprehensive list of patients
• Categorize type of breach for each patient
  • Some may be financial and require free credit report
  • Prepare your people or operators at a call center to be able to answer questions on what information was breached
• Find unique patients from that list
• Find their contact information

Typically your Corporate Responsibility, Legal and PR departments will handle media notification

Typically outside services will
• Print and transmit letters (organize by ZIP, etc.)
• Answer first-level calls with scripts
Encryption Issues

• Software
  – The graphical identification and authentication (GINA) library is a component of the operating systems that provides secure authentication and interactive logon. GINA’s starting in correct order. (Windows, Novell, Broadcom)
  – Application testing
  – Software updates to application and clients syncing to enterprise server.
  – I/O during boot up (roaming profiles)

• Hardware
  – More I/O done by BIOS, boot time impacts are different on different device types
  – Solid-state drive (SSD)
Solid-state drive (SSD)

- 5 potential reasons for slowdown complaints
  - Encryption software takes longer, but this isn’t observable because of the HD delays between sectors, seeks – there is no such delay for SSH, so all increased delay from encryption is easily observable
  - Buffer sizes for FDE may not be optimal for SSD; FDE may change default write size
  - SSD can only erase a line at a time, so sub-line sized writes may cause the SSD to reorganize multiple lines, causing extra “inexplicable” delay
  - 90 seconds just seems too long when you paid extra to get a machine that would boot in 20 seconds
  - SSD devices can only write each block so many times, so the device protects itself by proactively re-writing often updated blocks to a new location, causing more delay
Questions?

• This talk ends at 9:15
• Slides will be available from the SecureWorld Detroit website in a few days.

Larry.Yob@AscensionHealth.org
Scott.Aschenbach@StJohn.org