An Analysis of HIPAA Breach Data

Patrick Morrison, Laurie Williams
North Carolina State University
{pjmorris, lawilli3} @ ncsu.edu
http://www.realsearchgroup.org
“However beautiful the strategy, you should occasionally look at the results.”

– Winston Churchill
HIPAA Wall of Shame

Health Information Privacy

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Full DataSet [CSV format (18 KB)] [XML format (57 KB)]

Select a column head to sort by that column. Select again to reverse the sort order. Select an individual record to display it in full below the table.

Filter: 479 records showing

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Individuals Affected</th>
<th>Date of Breach</th>
<th>Type of Breach</th>
<th>Location of Breached Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accendo</td>
<td>AZ</td>
<td>175,350</td>
<td>2011-01-01</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper</td>
</tr>
<tr>
<td>Access Medical Group</td>
<td>PR</td>
<td>7,606</td>
<td>2012-01-11</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Adult &amp; Child Care Center</td>
<td>IN</td>
<td>550</td>
<td>2012-05-10</td>
<td>Hacking/IT Incident</td>
<td>Other</td>
</tr>
</tbody>
</table>
Example…

“Protected health information was released from the covered entity when an imposter, posing as representatives of the legitimate recycling service used by the covered entity, removed several barrels of purged x-ray films and film jackets.”
Breach Fields Reported

- Name of Covered Entity
- State
- Individuals Affected
- Date of Breach (Posted or Updated)
- Type of Breach
- Location of Breached Info
- Summary
Three Fields Considered

- **Breach Type**
  - e.g. ‘Theft’, ‘Loss’, ‘Hacking/IT Incident’

- **Breach Location**
  - e.g. ‘Laptop’, ‘Email’, ‘Backup tape’

- **Breach Summary**
  - Text description of breach (102 summaries/392 records)
## Results Table

<table>
<thead>
<tr>
<th>Breach Count Type/Location</th>
<th>Theft</th>
<th>Unauthorized Access/Disclosure</th>
<th>Loss</th>
<th>Hacking/IT Incident</th>
<th>Improper Disposal</th>
<th>Unknown</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>27</td>
<td>46</td>
<td>13</td>
<td></td>
<td>20</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Laptop</td>
<td>87</td>
<td>5</td>
<td>4</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer</td>
<td>51</td>
<td>10</td>
<td>4</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Portable Electronic Device</td>
<td>40</td>
<td>2</td>
<td>25</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Server</td>
<td>16</td>
<td>18</td>
<td>1</td>
<td></td>
<td>21</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>4</td>
<td>7</td>
<td>11</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Email</td>
<td>2</td>
<td>6</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Medical Record</td>
<td>4</td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>X-ray film</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup tape</td>
<td>1</td>
<td></td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compact Disc</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hard drive</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>235</td>
<td>98</td>
<td>62</td>
<td></td>
<td>35</td>
<td>23</td>
<td>6</td>
</tr>
</tbody>
</table>
Results Summary

- Theft, Loss, and Improper Disposal, combined, account for almost 70% of breach instances \((235+62+23)/461\).
- The most common media breached across Types was Paper, with 24% of breach instances \((109/461)\).
- Encryption is almost non-existent in reported breach instances.
Recommendations

- Disable the print button
- Encrypt PHI at its creation
  - (and decrypt only for use)
- Limit data on portable devices
Concerns...

- A reviewer observed that our recommendations were not novel; we agree.
- It appears that these ideas are not yet universally implemented.
- Consider the entire workflow, not just the software.
Surely there’s more we can do…

- How do we translate what is known about security and privacy into health care practice?
- Can we reshape the health care workflow through software design?
  - Can ‘The Cloud’ help limit the number of copies of PHI?
  - Could we encrypt what’s printed, and have providers wear ‘Decoder glasses’?
  - Your input is clearly needed here…
Thank You