One Size Doesn’t Fit All:
Lessons learned from recent HIPAA violations

Nate Steed and Danyale Phillips
Anchorage Comm. Mental Health Svcs.

- Non-profit organization.
- Experienced a breach—malware.
  - 2,743 individuals.
- Reported breach to HHS.
  - Led to an investigation.
Anchorage Comm. Mental Health Svcs.

- HHS Findings:
  - Never conducted a risk assessment.
  - Never implemented security policies and procedures.
  - Inadequate firewalls.
  - Ran outdated, unsupported software.
  - Failing to install patches.
- Outcome: $155,000 settlement, corrective action plan.
Cornell Prescription Pharmacy

- Small, single location pharmacy.
- Local news channel ran story about improperly disposed medical records.
  - 1,610 patient records in unlocked container.
- News channel reported story to HHS.
Cornell Prescription Pharmacy

• HHS findings:
  - No written privacy policies and procedures.
  - Did not train workforce.
  - Failed to adequately safeguard PHI.

• Outcome: $125,000 settlement, CAP.
St. Elizabeth’s Medical Center

• Tertiary Care Hospital in Brighton, MA.
  ▶ Medical practice using internet-based document-sharing application to store health records.
    › No business associate agreement requiring protection of the data.
    › No risk assessment performed.

• Settled HIPAA violation charges with HHS for $218,400.
New York and Presbyterian Hospital

- Had arrangement with Columbia University where CU staff acted as attending physicians to patients.
- CU physician had a server connected to the Hospital’s IT system.
  - Physician attempted to deactivate the server—left medical records on Hospital’s system accessible to internet search engines.
  - Error went undetected because Hospital did not analyze all systems that accessed Hospital’s system.
Feinstein Institute for Medical Research

• Biomedical research institute operated by a large, New York health system.
  ♦ Feinstein self-reported the theft of laptop containing 13,000 patient and research participant records.
    › Security management process was limited in scope.
• Settled HIPAA violation charges with HHS for $3.9 million.
North Memorial Health Care

• Not-for-profit healthcare system in Minnesota
  - NMHC self-reported the theft of laptop containing 9,497 records from a business associate’s workforce member’s locked vehicle.
    - No Business Associate Agreement in place
    - Incomplete risk assessment.

• Settled HIPAA violation charges with HHS for $1.55 million.
Lincare, Inc.

- Provider of respiratory care, infusion therapy, and medical equipment to in-home patients, operating in 48 states.
  - OCR received an individual complaint that a Lincare employee had left documents containing PHI of 278 patients after moving residences.
    - Inadequate policies and procedures to account for records taken offsite.
- Civil monetary penalties upheld for $239,800.
University of Washington Medicine

• Includes several entities under the control of University of Washington.
  ❧ UWM self-reported a breach affecting approximately 90,000 individuals.
    › Employee downloaded an email attachment that contained malicious malware.
    › Malware compromised the IT system and affected two groups of patients.

• Settled HIPAA violation charges with HHS for $750,000.
Cancer Care Group, P.C.

- Private physician practice with 13 radiation oncologists serving hospitals and clinics in Indiana.
  - CCG self-reported the theft of a laptop from an employee’s car containing information for 55,000 current and former patients.
    - Had not conducted an enterprise-wide risk analysis.
    - No policy specific to the removal of hardware and electronic media containing PHI.
- Settled HIPAA violation charges with HHS for $750,000.
Advocate Health Care Network

• Largest fully integrated health care system in Illinois.

• Self-reported 3 separate breaches:
  - Theft of 4 desktop computers (4 million records)
  - Breach of business associate (2,000 records)
  - Theft of unencrypted laptop (2,200 records)

• Advocate has agreed to settlement of $5.55 million
University of Mississippi Medical Center

- Mississippi’s sole public academic health science center and provides patient care for four specialized hospitals and clinics throughout the state.
- Password-protected laptop was missing from ICU.
  - Investigation indicated that it was likely stolen and the information for 10,000 individuals was likely compromised.
  - Further investigation revealed the network drive containing 67,000 files was also accessible.
- Settled HIPAA violation charges with HHS for $2,275,000.
Catholic Health Care Services of the Archdiocese of Philadelphia

• CHCS provided management and information technology services as a business associate to six skilled nursing facilities.

• Theft of company-issued iPhone
  • 412 individuals affected

• Settled HIPAA violation charges with HHS for $650,000

• First enforcement action against a business associate
Costs

• Factors **increasing** cost of breach
  - Lost or stolen devices (+$9)
  - Third party involvement (+$16)
  - Quick notification (+$8.90)
  - Consultants engaged (+$4.50)
Costs

• Factors **decreasing** cost of breach:
  ✷ CISO with enterprise-wide responsibility (-$5.60)
  ✷ Business continuity management (-$7.10)
  ✷ Incident response plan (-$12.60)
  ✷ Extensive use of encryption (-$12)
HIPAA Security Series

Security Standards Matrix (Appendix A of the Security Rule)

<table>
<thead>
<tr>
<th>Standards</th>
<th>Sections</th>
<th>Implementation Specifications (R)= Required, (A)=Addressable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process</td>
<td>§ 164.308(a)(1)</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sanction Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information System Activity Review</td>
</tr>
<tr>
<td>Assigned Security Responsibility</td>
<td>§ 164.308(a)(2)</td>
<td></td>
</tr>
<tr>
<td>Workforce Security</td>
<td>§ 164.308(a)(3)</td>
<td>Authorization and/or Supervision</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Workforce Clearance Procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Termination Procedures</td>
</tr>
</tbody>
</table>

http://www.hhs.gov/hipaa/for-professionals/security/guidance/
Questions?

Thank you!

Nate Steed
Warner Norcross & Judd LLP
nsteed@wnj.com

Danyale Phillips
Warner Norcross & Judd LLP
dphillips@wnj.com

These materials are for educational use only. This is not legal advice and does not create an attorney-client relationship.