HIPAA PRIVACY ...

One Year Later

HCCA Compliance Institute 2004

Chicago, Illinois  April 27, 2004

John E. Steiner, Jr., Esq.
Chief Compliance Officer and Privacy Officer
The Cleveland Clinic Health System
Cleveland Clinic Health System

The Cleveland Clinic Foundation
• Not-for-profit, multispecialty academic medical center that integrates clinical and hospital care with research and education.

• Founded in 1921, based on not-for-profit group practice model.

Lerner Research Institute
Cleveland Clinic Health System
Campuses in Ohio and Florida
HIPAA Privacy Preamble, Rulemaking and Office for Civil Rights (OCR) Guidance repeated reference to “reasonableness,” for example:

- Good faith efforts to issue Notice of Privacy Practices
- Physical, Administrative, and Security Safeguards
- Communication of Protected Health Information between treating physicians
- Training obligation of Covered Entities
• HIPAA Project Management Office
• Privacy Official for each region
• Regulation specific teams established:
  - Transactions
  - Privacy
  - Security
• Monthly meetings of Privacy Office, including Legal Counsel
PRIVACY - SCOPE

- Consumer control of information
- Patient privacy rights defined
- Boundaries on Medical Record usage
- Access controls to information
- Security measures for patient information
- Assignment of Privacy Officer by Region
- Business Associate contracts database
25,000+ employees to train/educate on HIPAA regulations

- Audience types to be defined
- Develop approach and plan based on employee type
  - Multiple approaches used
- ID/Inventory trainees
- Training material and media: videotape and cbt module
<table>
<thead>
<tr>
<th>Name of Organization</th>
<th>Policies</th>
<th>Procedures</th>
<th>Training/Educ</th>
<th>Businesss Associates</th>
<th>Implementation</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
HIPAA Overview

HIPAA Privacy Rule

- HIPAA privacy rules give specific rights to patients

- Healthcare providers cannot:
  
  Use or disclose Protected Health Information (PHI) without the acknowledgement and/or consent of the patient or as permitted by the regulations.
Use = the release of PHI within the covered entity for “treatment, payment, or health care operations” (TPO).

Disclosure = the release of PHI outside of the covered entity for TPO
Patient Rights

The HIPAA Privacy Rule creates patient rights specific to Protected Health Information

1. Accounting of Disclosures (See: AHA letter)
2. Access to PHI
3. Amendments to PHI
4. Confidential Communications
5. Restriction of Use or Disclosure of PHI
Patient Rights: Amendments to PHI

- Must be in writing and sent to the medical records department.
- Amendment requests with clinical implications, versus objective criteria, must go through a special process.
Patient Rights: “Restrictions”

- Most patients are not aware of the limitations on this Privacy right.

- There are broad “carve outs” from Restrictions for uses of PHI for “treatment, payment, or health care operations.” There also are special rules for restrictions on disclosures.

- The regulatory commentary to Section (a)164.522 includes these points:
“While a covered entity is not required to agree to such restrictions, it must act in accordance with any restrictions it does agree to. Failure of a covered entity to act in accordance with any agreed to restriction is a violation of the Privacy Rule.”
Patient Rights: “Restrictions”

“Notwithstanding an agreement to restrict between the covered entity and the patient, a covered entity may use or disclose the restricted information needed for a patient's treatment in an appropriate medical emergency, or when the use or disclosure without the patient’s written permission is authorized or required by law.”
FDA Related Activities

Covered entity may disclose Protected Health Information for FDA related activities, including monitor visits.

Medical Research Issues
HIPAA Privacy Rule
“A covered entity may end an agreement to restrict the use or disclosure of a patient’s PHI at any time by notifying the patient in writing. If the patient agrees with the covered entity’s decision to end the restriction, the PHI is no longer subject to the restriction. If the patient disagrees with the covered entity's decision, then the covered entity’s termination of the restriction only applies to PHI created after the covered entity gave the patient the written notice of termination of the restriction.”
Protected Health Information

• Incidental Use & Disclosures of PHI

A secondary use or disclosure that:
  - Cannot be reasonably prevented
  - Is limited in nature
  - Occurs as a result of another use that is permitted by the rule

See: Guidance from DHHS; Office of Civil Rights
Re: Federal Privacy Rule
December 3, 2002
“Incidental Uses and Disclosures” pp. 12-18

www.hhs.gov/ocr/hipaa
Protected Health Information

- Incidental Use & Disclosures of PHI
  - Computer monitors
  - Sign-in or out lists
  - Charts
  - Palm pilot
  - Insurance cards
  - Wrist bands
  - Clipboards
  - Charge tickets
  - Medication bottles
Privacy Practices

• Acknowledgment and Consent
  • In general, the covered entity will attempt to obtain acknowledgment and consent signatures prior to providing treatment.

  • There are exceptions to obtaining acknowledgment and consent prior to providing treatment:
Privacy Practices

• Exceptions to Acknowledgment and Consent

  ➤ Indirect treatment relationship
    - Reference laboratory tests
    - Radiology film review
    *The covered entity does not have face to face contact with the patient; however, provides expertise to another provider.*

  ➤ Emergency treatment situations
    - Patient must be stabilized
    *Acknowledgment and Consent can be obtained as soon as reasonably practical*
Privacy Practices

• Exceptions to Acknowledgment and Consent
  ✅ Good faith efforts following patient refusal to sign
    - Assumed; not necessary to get written consent.
    - Document good faith efforts.

  ✅ Discretion of a designated supervisor
    - CCHS policy is to have a designated supervisor
      or Ombudsman Office, talk with a patient who refuses
      to sign the Acknowledgement and Consent form.

    - The discussion should be documented.
Why Security Is Important

What Types of Security Breaches Have Been Experienced (Past 12 Months)?

<table>
<thead>
<tr>
<th>Breach Type</th>
<th>Percent of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of Proprietary Information</td>
<td>$70,195,900</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>65,643,300</td>
</tr>
<tr>
<td>Virus</td>
<td>27,382,340</td>
</tr>
<tr>
<td>Insider Abuse of Internet Access</td>
<td>11,767,200</td>
</tr>
<tr>
<td>Financial Fraud</td>
<td>10,186,400</td>
</tr>
<tr>
<td>Laptop Theft</td>
<td>6,830,500</td>
</tr>
<tr>
<td>Sabotage</td>
<td>5,148,500</td>
</tr>
<tr>
<td>System Penetration</td>
<td>2,754,400</td>
</tr>
<tr>
<td>Active Wiretap</td>
<td>705,000</td>
</tr>
<tr>
<td>Telecom Fraud</td>
<td>701,500</td>
</tr>
<tr>
<td>Unauthorized Insider Access</td>
<td>406,300</td>
</tr>
<tr>
<td>Telecom Eavesdropping</td>
<td>76,000</td>
</tr>
</tbody>
</table>

The Financial Impact
Total losses by type of attack

Likely Sources of Attack (1999 - 2001)

<table>
<thead>
<tr>
<th>Source</th>
<th>Percent of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreign Corp.</td>
<td></td>
</tr>
<tr>
<td>Foreign Gov.</td>
<td></td>
</tr>
<tr>
<td>U.S. Federal</td>
<td></td>
</tr>
<tr>
<td>Competitors</td>
<td></td>
</tr>
<tr>
<td>Disgruntled Employees</td>
<td></td>
</tr>
<tr>
<td>Independent Hackers</td>
<td></td>
</tr>
</tbody>
</table>

Business Sector Hack Targets 1/1/03 - 3/31/03

<table>
<thead>
<tr>
<th>Sector</th>
<th>Percent of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail</td>
<td>36%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>9%</td>
</tr>
<tr>
<td>Financial &amp; Insurance</td>
<td>12%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>9%</td>
</tr>
<tr>
<td>Services</td>
<td>22%</td>
</tr>
<tr>
<td>Gov't Federal</td>
<td>3%</td>
</tr>
<tr>
<td>Other</td>
<td>7%</td>
</tr>
</tbody>
</table>

Source: CSI/FBI Cybercrime Survey, 2003
Source: Security Magazine Survey, 2002
HIPAA Security

• HIPAA Security is about protecting Electronic Protected Health Information, whereas HIPAA Privacy is about all forms or Protected Health Information, including paper records.

• Enforcement agency is not defined in the Security Rule.
HIPAA Security Standards

• Administrative Safeguards (55%)
  12 Required, 11 Addressable

• Physical Safeguards (24%)
  4 Required, 6 Addressable

• Technical Safeguards (21%)
  4 Requirements, 5 Addressable

The final rule has been modified to increase flexibility as to how protection is accomplished.
Administrative Safeguards

• 50% of the Security Regulations requires Policies and Procedures for:
  - Day-to-Day Operations
  - Worker Conduct With PHI
  - Safeguard Selection, Deployment, & Management
Physical Safeguards

• Meant to Protect Information Systems & Facilities From:
  - Natural Disasters
  - Environmental Hazards
  - Unauthorized Intrusions

• Contains Admin Policies & Physical Controls
Technical Safeguards

• Specifies How to Use Technology To:
  - Protect PHI
  - Control Access to PHI
Benefits

• Establishes Minimum Baseline
• Encourages the Use of Electronic Data Interchange (EDI)
• Promotes Connectivity/Provide Availability of Information
• Reduces the Risks & Potential Cost of a Security Incident
To Do List

• Assign Security Responsibility to **One Person**
• Formalize **Program Management Office (PMO)**
• Conduct a Risk & Gap Analysis
• Select & Document - People, Process, & Tool Investments
• Develop/Deliver **Training, Education & Awareness** (TEA)
• Develop Policies & Procedures
• Review & Modify Access & Audit Controls
• Establish Security Incident Reporting & Response Plan
• Develop the Compliance Scorecard
How Does This Affect You?

You Need to Know:
• Who is Responsible for Information Security
• Who can Answer Your HIPAA Questions (Privacy or Security)
• Where to Find the Security Policies
  http://intranet.cchs.net/policies/hipaa/
• The Content of Existing & New Security Policies
• How to Report an Incident

You May Need to:
• Deliver Department or Job-Specific Training
• Follow Some New Procedures
Real World with HIPAA

A Provider’s Quick Reference Guide to those confusing daily Privacy issues!

Which family members or friends can I talk to about the care of a patient?
You may discuss the patient’s care with any person who is a family member or friend of the patient who is involved in the patient’s care or payment for that care, so long as the patient has had the opportunity to object to that person and has not done so. If the patient is unable or unavailable to object, you will need to use your professional judgment to determine if discussing the patient with the person is in the patient’s best interest.

How do I verify that a caller/person is a friend or family member with whom I can share information?
Since you may not always know who all of the friends and family are, you should initially rely on the patient. If the patient gives you permission to discuss his or her care with someone who is there in person, then no further verification is needed. However, handling of phone calls is more difficult. You should use some method of verifying that the person you are speaking with is legitimately entitled to information about the patient. Some
Office of Corporate Compliance & Privacy Office
The Cleveland Clinic Health System

Summary of HIPAA Enforcement Authority
and Enforcement Posture
(as of October 2003)

By: John E. Steiner, Jr., Esq.
Chief Compliance Officer and Privacy Official

Background
This memorandum summarizes key legal authorities from the HIPAA statute, regulations, and guidance from regulatory agencies regarding the above topic. This memo does not address whether or how a private party might seek to use any HIPAA standards in a private, civil lawsuit; although there is strong speculation that such an eventuality will occur.

From the federal government perspective, the following agencies are responsible for HIPAA
HIPPA Security –
One Year and Counting

American Hospital Association

Security Rule Implementation Issues
Melinda Reid Hatton
Vice President and Chief Washington Counsel
HCCA’S 2004 Annual Compliance Institute
April 27, 2004
Current Challenges

• **Getting Paid**
  • Continuing focus on making HIPAA standard transactions work

• **HIPAA burnout**
  • Just finished privacy and still focused on Transactions and Code Sets (TCS)
  • May be behind in security efforts

• **Didn’t we already do this for privacy compliance?**
Enforcement Concerns

- **Enforcement must be consistent with flexible, scalable approach in final rule**
  - Security breach is not same as rule violation
  - No second guessing of risk calculus, decision
- **Overlap between privacy security**
  - Office of HIPAA Standards v. OCR
- **Consistency in interpretation**
  - Central Office v. Regional Offices
Other Provider Worries

• Security rule fueling technology purchases
  • Long repressed technology wish lists
  • Consultant, vendor misinformation, scare tactics
  • False sense of security from technical solutions
Survey Results

- AHA conference call survey
- Results based on 475 organizations
- Caveat: Not random sample!
Stage in Implementation and Compliance

Not Started: 1.4%
Initial Research: 43%
Planning Stage: 46.8%
Risk Assessment/Evaluation: 43%
Implementation Stage: 25.7%
Compliant: 9.3%
Other: 2.1%
Has Privacy Focus Been an Obstacle in Security Implementation?

- No: 69.8%
- Yes: 27.6%
- Other: 2.6%
Has TCS Focus Been an Obstacle in Security Implementation?

Percentage Response:
- No: 64.8%
- Yes: 33%
- Other: 2.1%
Have There Been Any Other Obstacles in Security Compliance?

- No: 36.5%
- Yes: 63.5%

Percent Response
Listed Obstacles in Security Compliance

- Lack of Budget/Resources
- Time / Multiple Priorities
- Competing IS Projects
- Misinformation/Unclear Guidance
- IT Security Education/Training
- Sheer Scope of Project
- Finding Good Security Policies
- Complexity of Organization
- IT/IS Staff Turnover
- Outsourcing IT/IS Department
- Lack of Agreement on Scope and Depth of Required Security Regulation Implementation…
Has Organization Budgeted for Security Rule Implementation?

- No: 34.5%
- Yes: 55%
- Other: 10.5%

Percent Response
Resources To Be Used For Security Rule Implementation?

- Internal and External: 62.1%
- External Only: 5.2%
- Internal Only: 25.7%
- Other: 6.9%

Percent Response
AHA Resources

• AHA HIPAA website:  www.aha.org
• AHA audio conferences
• AHA endorsement of Ernst & Young
  • As HIPAA security strategic advisor – services include risk analysis, gap assessment and all security implementation services
  • joint advisories, checklists, briefings and other documents for AHA members
• Representation, as needed through implementation