HIPAA Privacy, Security, Breach, and Meaningful Use
Practice Requirements for 2012

CHUG October 2012
Standards for Privacy of Individually Identifiable Health Information (2003)
• Define and limit the circumstances in which an individual’s protected health information may be used or disclosed

• Applies to electronic protected health information (EPHI)

• Standardized language by which transactions are made

HIPAA Administrative Simplification (2006)
• Civil Penalties, Notification of Public, NPI’s, Standards for claims and codesets

HITECH (Health Information Technology for Economic and Clinical Health 2009)
• Breach Notification Rule establishes first national security breach notification law
• CRIMINAL Enforcement

Affordable Care Act (2010)
• Accelerates the timelines for adoption of standards
Requires HHS to provide periodic audits to ensure covered entities and Business Associates (BA) are complying with the HIPAA Privacy and Security Rules and Breach Notification standards.

- Audits will no longer be driven by responses to complaints or breaches,
- Audits will be directed at organizations that Office of Civil Rights (OCR) selects based on an overall risk profile (e.g., size, type, complexity),
- In 2011, the OCR in awarded a $9.2 million contract to KPMG to administer the HIPAA privacy and security compliance audits,
- The first phase of the audits began in Fall 2011,
- Medicare (through its contractors) will audit MU,
- Business Associates will be included in future audits.
• Permits States’ Attorneys General to bring civil actions on behalf of state residents. Cost of suit and attorneys fees can be awarded,
• Gives consumers’ rights to an accounting of disclosures,
• Heightened enforcement,
• Limits disclosures for marketing and fundraising,
• Prohibits the sale of protected health information,
• Requires covered entities to notify patients whose PHI is compromised by a “breach”.

HITECH
### HITECH Authorized Criminal Penalties

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Criminal Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowingly obtain or disclose individually identifiable health information</td>
<td>Up to $50,000, as well as imprisonment up to one year</td>
</tr>
<tr>
<td>Offenses committed under false pretenses</td>
<td>$100,000 fine, with up to five years in prison</td>
</tr>
<tr>
<td>Committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit</td>
<td>$250,000, and imprisonment for up to ten years</td>
</tr>
</tbody>
</table>

- Providers, staff, Business Associates, and corporate officers are at risk,
- If not an individual covered under HIPAA, may be charged with Conspiracy or Abetting.
<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to reasonable cause and not due to willful neglect</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected within the required time period</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to willful neglect and is not corrected</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>
Since April 2003, HHS has received 72,684 HIPAA complaints. 17,025 have resulted in remediation and/or fines. (Aug 29, 2012)

Most frequent findings:
- Impermissible uses and disclosures of protected health information,
- Lack of safeguards of protected health information,
- Lack of patient access to their protected health information,
- Uses or disclosures of more than the Minimum Necessary protected health information and
- Lack of administrative safeguards of electronic protected health information.

OCR publishes their audit focus each year:
- Breach incident detection and response (OCR’s top issue),
  - Policies that define actions a covered entity will take,
- Access logging and review,
  - User access and passwords management,
  - Policies in how employees are retired.
- Theft or loss of mobile devices,
- Protective software.
EMR 2012 SECURITY BREACHES/PORTABLE DEVICES

• During 2009-2011, there were more than 19 million EMR security breaches,

• In 2011, the number of total records breached increased by 97% compared to 2010,

• Records breached due to loss of unencrypted devices by employees increased 525% in 2011,

• 60% of all breaches were the result of malicious intent including hackers, insider IT incidents, and theft.

• Epidemic enormity attributed to portable devices.
Meaningful Use
Meaningful Use (MU) Audits

- Formally began Spring 2012,
- Looking for demonstration of MU,
- Will require documentation,
- One Measure out of compliance will result in Stimulus dollar recoupment,
- “Conduct or review a security risk analysis ...implement security updates as necessary and correct identified security deficiencies as part of ...risk management”.
MU Audits

• Practices that receive an Audit letter have two weeks to reply,
  • Figloiozzi and Company, as the Department of Health and Human Services (HHS) Secretary's designee

• The letters ask physicians to provide three things;
  • Proof that the EHR system used to meet meaningful use requirements is certified,
  • Supporting documentation proving that core objectives were met,
  • Supporting documentation that so-called menu objectives were met.

• A report from your EHR system that ties to your attestation

• Do not inadvertently send PHI
Preventing Audits

• Are random today,
• Avoid attestation incongruencies;
  • Simple typos (non registered address),
  • Significantly differences in unique patients numbers,
  • Reporting less patient encounters than submitted already to CMS,
  • Claiming numerous exemptions,
  • Claiming exemption for “State unable to accept” while other providers attest that they have tested with the State,

Confucius: *Success depends upon previous preparation, and without such preparation there is sure to be an audit.*
Privacy
Privacy Rules

- Applies to all forms of patients’ protected health information, whether electronic, written, or oral,
- Requires covered entities to have in place appropriate:
  - Administrative
    - Written policies, documented training, sanctions, Privacy Notices,
  - Physical
    - Protected printers, Fax coversheets, computer screens, chart rooms,
  - And technical safeguards
    - Log out, secure transfer, encryption
- Gives patients the right to access their health care information, in the manner they request it,
- Gives the patient the right to rescind authorization to use or share their information.
What is Protected?

“Individually identifiable health information” is information, including demographic data, that relates to:

- Past, present or future physical or mental health or condition, (any dates of care),
- Past, present, or future payment for the provision of health care to the individual,
- Identifying the individual or for which there is a reasonable basis to believe can be used to identify the individual,
- Common identifiers (e.g., name, address, birth date, SSN, Drivers License.)
Where is PHI?

**Face to Face Conversation**
- Friends, Family, Acquaintances
- Co-Workers
- Patients, Clinicians
- Business Associates
- Clients

**Facsimile**
- Business Associates
- Clients
- Payors, Clearinghouses
- Employers, Attorneys

**Traveling Employees**
- Conversation
- Phone Conversations
- Paperwork
- Monitor Screens
- Disks and CDs
- Laptop Files

**Telephone**
- Friends, Family, Acquaintances
- Co-Workers
- Payors, Clearinghouses
- Business Associates
- Clients
- Patients
- Clinicians

**Home Offices**
- Paperwork
- Monitor Screens
- Computer Files
- Phone Conversations
- Disks and CDs

**Monitor Screens**
- Visitors
- Co-Workers
- Business Associates

**Paperwork**
- Desktops
- Printers, Copiers
- Files
- Trash Cans
- Meeting Areas

**Mail**
- Payors, Clearinghouses
- Clients
- Employers, Attorneys
- Business Associates
- Patients

**Internet**
- Friends, Family, Co-workers
- Payors, Clearinghouse
- Email
- Web pages
“A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations”

- May disclose to another provider or insurance carrier,
- **Authorization required: Psychotherapy notes.**
  - Except to carry out the following treatment, payment, or health care operations,
- May use for training purposes,
- To defend the entity in a legal action,
- Authorization is required for any marketing purposes.
The covered entity must provide a notice that is written in plain language and that contains these elements prominently displayed:

“THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY “
Minimum Necessary Requirements

- A Covered Entity (CE) must implement policies and procedures that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure,

- A CE must limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought.
Patient Rights

- Obtain an access report that lists those within an organization who have accessed their electronic records,
- Patient may give written or oral objection to a use or disclosure information:
  - Practice may not share with registries, insurers, other providers, family members, etc.,
  - Self-pay. You may bill the patient or require up front payment,
- Personal Representatives to share information with,
- Access to electronic health care information.
Privacy To-Do List

• Implement policies that explain:
  • What protected health information can be disclosed,
  • What can be faxed,
  • How to release information,
  • Who in your practice has access to what information,
  • How you would remediate any policy violation.

• Assign a formal HIPAA Privacy Officer. Document their duties.

• Train and document with sign in sheets,
• Maintain HIPAA folders and manuals,
• Maintain any documents regarding complaints or violations.
Security
Security Rule

- Technology neutral and scalable,
- Requires appropriate administrative, physical and technical safeguards,
- The rule requires that we “Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.”
- 45 CFR 164.305(b)(2) defines the following as factors to be aware of as you are assess and implement the security rules:
  - The size, complexity and capability of the covered entity
  - The covered entity technical infrastructure, hardware, and software security capabilities
  - The costs of security measures
  - The probability and criticality of potential risks to ePHI.
Technical Safeguards

- Virtual or Dedicated Firewall,
- Backup,
- Antivirus,
- OS Patch Management,
- Encryption is not required but it is strongly suggested,
- Document data management, security, training and notification plans,
- Secure password use,
- Only use secure access for remote access.
Security To Do

- Perform and document a Gap Analysis/Risk Assessment to identify and remediate risks,
- Implement policies and procedures to prevent, detect, contain, and correct security violations,
- Train all staff,
- Monitor and audit your network,
- Prepare for and manage any attack or compromise.

*OCR expects that organizations are performing routine Gap Analyses. Meaningful Use requires an annual Risk Assessment.*
Breach Rules
“Breach” means unauthorized access, acquisition, use or disclosure of protected health information which compromises the security or privacy of that information.

• Paper or electronic,
• There are three exceptions to the definition of breach:
  • Unintentional access by a coworker,
  • Inadvertent disclosure to another healthcare worker,
  • Good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.
Breach Notification Requirements

Covered entities must provide notification of the breach to (1) affected individuals, (2) the Secretary, and, in certain circumstances, to (3) the media.

- Provide individual (every patient) notice in written form by first-class mail,
  - Provide without unreasonable delay and in no case later than 60 days,
- A breach affecting more than 500 patients requires a notice to prominent media outlets serving the State or jurisdiction (press release),
- Notify the Secretary by completing a report on the HHS web site,
- If a breach occurs by a business associate (BA), the CE manages the breach,
- The CE has the “burden of proof” to demonstrate that all required notifications have been provided,
- Must have in place written policies and procedures, train employees and procedures, and develop appropriate sanctions.
Daily Breach News

- IHealthBeat  Monday, August 20, 2012
  - M.D. Anderson Alerts 2,200 Patients About Recent Data Breach,
- HealthCare IT News Monday, August 20, 2012
  - Former employee arrested after FBI investigation into hospital security breach DXX MXXXXe is accused of accessing more than 700,000 patient records in two years and then selling them for social security numbers,
- Little Rock. Arkansas April 24th, 2012
  - The University of Arkansas for Medical Sciences-Physician emailed PHI,
- July 2012 Beth Israel Deaconess Medical
  - 3900 patients will be getting letters alerting them that some of their personal health information may have been breached after a physician’s personal laptop computer was stolen
- 3/13/2012: Blue Cross Blue Shield of Tennessee pays $1,500,000
  - Agrees to a corrective action plan to address gaps in its HIPAA compliance program. Theft of a computer hard drive containing PHI.
## 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: university 44 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</th>
</tr>
</thead>
<tbody>
<tr>
<td>Georgetown University Hospital</td>
<td>DC</td>
<td>2,416</td>
<td>2010-03-26</td>
<td>Theft</td>
<td>Email, Portable Electronic Device</td>
</tr>
<tr>
<td>Johns Hopkins University Applied Physics Laboratory Medical and Dental Insurance Plan</td>
<td>MD</td>
<td>632</td>
<td>2016-02-17</td>
<td>Unauthorized Access/Disclosure</td>
<td>Flash Drive</td>
</tr>
<tr>
<td>Loma Linda University Health Care</td>
<td>CA</td>
<td>591</td>
<td>2010-04-01</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>Loma Linda University School of Dentistry</td>
<td>CA</td>
<td>10,100</td>
<td>2010-06-13</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>New York Presbyterian Hospital and Columbia University Medical Center</td>
<td>NY</td>
<td>6,800</td>
<td>2010-07-01</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>The University of Texas at Arlington</td>
<td>TX</td>
<td>27,000</td>
<td>2010-02-10</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Thomas Jefferson University</td>
<td>PA</td>
<td>21,000</td>
<td>2010-05-14</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
</tbody>
</table>
Breaches

• **YES**
  - Incorrect papers given to a patient,
  - Incorrect bill, results, or reminder sent to a patient,
  - Lost or stolen Phone, hard drive, laptop, etc. that contains PHI,
  - Employee viewing charts they should not be accessing,
  - Failure to sign a BAA and allow consultant to work,
  - Patient chart is stolen from a health care provider’s car,
  - Complete loss of a medical record.

• **NO**
  - Chart copies found in local trash before being disposed of,
  - Internal email with PHI to wrong staff member,
  - The plumber is talking to a manager with PHI on monitor screen.
Risk Assessment
Risk Assessment Process

- Evaluate
- Identify Issues
- Assess Impact
- Repair
- Policies and Training
- Monitor and Re-do

Example Checklist

The Office of the National Coordinator has posted a Guidance for Practices:

### Breach Risk Assessment Questions

<table>
<thead>
<tr>
<th>Potential Breach Point</th>
<th>Potential Scenario</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHI stored in X</td>
<td>Lost key or potentially left unlocked.</td>
<td>Low risk. File is in internal ... Check cabinet at end of day. Have cabinet rekeyed if keys are lost.</td>
</tr>
<tr>
<td>EPHI stored on Servers</td>
<td>Information is hacked (by employee or outside source)</td>
<td>Encrypt data with X tool. Encryption will provide safe harbor.</td>
</tr>
<tr>
<td>PHI sent via U.S. Mail</td>
<td>Item is lost in the mail</td>
<td>Minimal impact if only 1 item sent at a time, but still needs to be reported as a breach. If more than 25 items, use Fed Ex direct signature service.</td>
</tr>
<tr>
<td>PHI sent via Fax</td>
<td>Item sent to wrong fax number</td>
<td>Minimal impact if only 1 item sent at a time, but still needs to be reported as a breach.</td>
</tr>
<tr>
<td>Items sent via HTTPS using vendor web site</td>
<td>Vendor site is hacked or experiences problems</td>
<td>Out of our control; must work with vendors to address</td>
</tr>
<tr>
<td>PHI received from employees</td>
<td>Employee sends via interoffice mail instead of hand deliver</td>
<td>All employees sign confidentiality agreements; should not be considered as breach.</td>
</tr>
</tbody>
</table>
Sample Policies – Available online

New Policies May Be Needed:
  - Release of *electronic* records,
  - Definition of patient summaries,
  - Use of Phones to access PHI,
  - Breach prevention,
  - Wireless network security,
  - Ongoing HIPAA monitoring.
## HIPAA Training Sign Up Sheet

**Dr Joe**

5/1/2012 10:00

<table>
<thead>
<tr>
<th>Name</th>
<th>Yes I Attended Training (X)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>
HIPAA Privacy, Security, or Breach Audits
Internet search for “HIPAA Complaint” returns 1+ million results

#1 Response is:

Here is the online form:

[Image of online form]

Here is the online form:
OCR Complaint Process

H Hippa Privacy & Security Rule Complaint Process

Complaint

Intake & Review

Possible Criminal Violation

Possible Privacy or Security Rule Violation

DOJ

Accepted by DOJ

Resolution

OCR finds no violation
OCR obtains voluntary compliance, corrective action, or other agreement
OCR issues formal finding of violation

Resolution

The violation did not occur after April 14, 2003
Entity is not covered by the Privacy Rule
Complaint was not filed within 180 days and an extension was not granted
The incident described in the complaint does not violate the Privacy Rule
Initial Response to Any HIPAA Complaint

Take NO action until these steps are complete:

- Determine potential number of patients that could be involved,
- Document and save all facts known,
- Interview all involved parties and document,
- Determine if there is a CMS or OCR complaint on file,
- Meet with senior staff and your Privacy and Security Officers,
- If concerns of potential harm to a patient, meet with your attorney,
- Gather all of your HIPAA policies, folders, risk assessment, and documentation.
If You Identify a Breach

• Determine extent of breach
  • If greater than 500 patients, involve your attorney,
  • If more than 10 patients cannot be reached, involve your attorney,

• Follow Initial Complaint Process (previous slide)

• Then:
  • If less than 500 patients involved:
    • Identify issue, document all facts,
    • Take remedial action,
    • Notify HHS, including remedial actions,
    • Notify patient by call or certified mail.
• Advanced notice before any audits,
  • Can be 2 business days,
• Site visits will include:
  • Interviews with leadership,
  • Examination of offices and operations,
  • Policy and documentation review,
  • Observation of compliance with your policies.
• Post visit audit reports:
  • Raw data collection materials such as completed checklists and interview notes,
  • Specific recommendations for actions,
  • Recommendations to the OCR regarding continued need for corrective action.
HHS HIPAA Audit Timelines

1 Day  
Notification letter sent to Covered Entities

Minimum of 10 Days  
Receiving and Reviewing Documentation and Planning the Audit Field Work

3 – 10 Days  
Onsite fieldwork

20 – 30 Days  
Draft Audit Report

10 Days  
Covered Entities Review and Comment on Draft Audit Reports

30 Days  
Final Audit Report

Elapsed Time

References to days are in business days.
After the Audit

- Audits are primarily a compliance improvement activity,
- OCR will review the final reports, including the findings and actions taken by the audited entity,
- Generally, OCR will use the audit reports to determine what types of corrective action are most effective,
- For a serious compliance issue, OCR may initiate a full compliance review. This could include other agencies with civil and criminal enforcement authority,
- Complete and document any actions recommended to close the case.
Recently Managed Cases

• Left too much information on answering machine,
• Sent entire record to disability company,
• Failed to provide appropriate Privacy Notice prior to treatment,
• Overcharged for providing records,
• Gave information to media, employer, or school,
• Allowed others access to computer screen in waiting room,
• Failed to have appropriate BAA signed,
• Release other information to Workers’ Comp carrier,
• Sent EOBs/Statements to wrong persons,
• Denied access to records.
Typical Remediation

- A lot of “red tape”,
- Develop new policies,
- Implement new safeguards,
- Re-train staff. Document training,
- Sanction responsible staff member,
- Review past actions and remediate,
- Apologize in writing,
- Fines and potential criminal charges,
- Make findings public.
Fun FAQs

• Can I still Fax?
• Can I email?
• What can I say to family members?
• Can I send appointment reminders, etc?
• Can I have sign in sheets?
• Can my Drug Rep have access to our patient information?
• What if my BA makes a disclosure?
• Does the cleaner, plumber, etc. need a BAA?
• Can I release a patient record with family history?
• Can I have a chart on the patient’s door?
• Can I be sued?
Thank You
Paula Infeld, RN, CPHIMS
Sage Growth Partners
pinfeld@sage-growth.com