Objectives

- Identify the purpose of HIPAA regulations
- State key privacy and security changes for your practice resulting from the American Recovery and Reinvestment Act (ARRA) of 2009
- Name two breach notification requirements and explain consequences of a violation
- Discuss key changes to HIPAA based on the Omnibus Rule
In the News: HIPAA Fines

- Alaska DHHS fined $1.7 million
  - USB device stolen from employee vehicle
- Cignet Health fined $4.3 million
  - Failure to provide medical records to 41 patients
- UCLA fined $865,500
  - Snooping employees
- CVS fined $2.25 million
  - Disposal of PHI in trashcans
- Blue Cross of Tennessee fined $1.5 million
  - Unencrypted laptops stolen

Department of Health and Human Services, May, 2011
HIPAA Violations on the Rise…

• In the last three years, over 70,000 HIPAA violation complaints filed
• Majority of breaches: theft, loss, or unauthorized access or disclosure (i.e. by employees)
• Greatest vulnerability in mobile devices: phones, tablets, laptops, desktops
Purpose of HIPAA

• Health Insurance Portability and Accountability Act (HIPAA) of 1996
  ▪ Protect individuals’ rights to privacy and confidentiality
  ▪ Assure the security of electronic personal information

• Privacy Rule assures individuals’ health information is properly protected, while allowing the flow of health information to promote care
Health Insurance Portability and Accountability Act (HIPAA)

• Key Components:
  ▪ Protected Health Information (PHI): “All individually identifiable health information transmitted or maintained by a covered entity, regardless of form”
  ▪ Covered Entity: “A health plan, healthcare clearinghouse, or healthcare provider who transmits any health information in electronic form in connection with a standard transaction”
  ▪ Patient Rights
# PHI 18 Identifiers

<table>
<thead>
<tr>
<th>PHI 18 Identifiers</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical record number</td>
<td>Name</td>
</tr>
<tr>
<td>Health plan beneficiary number</td>
<td>Postal address</td>
</tr>
<tr>
<td>Device identifiers and serial numbers</td>
<td>All elements of dates except year</td>
</tr>
<tr>
<td>Vehicle identifiers and serial numbers</td>
<td>Telephone number</td>
</tr>
<tr>
<td>Biometric identifiers (i.e., finger and voice prints)</td>
<td>Fax number</td>
</tr>
<tr>
<td>Full face photos and other comparable images</td>
<td>E-mail address</td>
</tr>
<tr>
<td>Any other unique identifying number, code, or characteristic</td>
<td>URL address</td>
</tr>
<tr>
<td>IP Security</td>
<td>Social Security number</td>
</tr>
<tr>
<td>Account numbers</td>
<td>License numbers</td>
</tr>
</tbody>
</table>
State Law and HIPAA

- State privacy laws can be more stringent than HIPAA regulations
- In this case, state laws are followed
- Otherwise, HIPAA regulations are followed
HIPAA Scenario #1

Dr. Jones, head of surgery, asks to see Kristi Smith’s chart. Dr. Jones is not Kristi’s physician but Kristi is his wife’s best friend and he wants to see how she is doing. What do you do?

a. Give Dr. Jones the chart.
b. Ask Dr. Jones for appropriate written authorization to review Kristi’s chart.
c. Tell Dr. Jones that he cannot see the chart since he is not the patient’s physician.
d. Tell Dr. Jones you are too busy to get the chart.
ARRA, aka “Stimulus Bill”

- Signed into law February 17, 2009
- Title XIII
- Expands the scope of HIPAA
- Changes how business associates are handled
- HITECH Act
  - Develops standards for electronic exchange and use of health information
  - Investment of $20 billion in HIT
  - Savings of $10 billion in quality improvement and care coordination
  - Strengthens privacy and security of PHI
ARRA Definitions

• Covered entity, business associates, and protected health information (HIPAA definitions)
• Electronic health records
• Breach
• Personal health record
Final HIPAA Omnibus Rules Require Attention

- Modifies HIPAA privacy
- Adopts changes to the HITECH Act
- Supplants interim final Breach Notification Rule
- Updates to BA agreements
HIPAA Scenario #2

Which of these facts about the HIPAA Omnibus Rule is false?

a. The rule is 563 pages long.
b. The proposed rule was first released in July 2010, reached the Office of Management and Budget by March 2012, and was finally released on January 17, 2013.
c. The Office of the National Coordinator for Health Information Technology (ONC) released the rule.
d. The rule went into effect March 26 and covered entities have until September 22, 2013 to get into compliance.
HIPAA Omnibus Rule Penalties

• Additional enforcement power
• New Penalty System under HIPAA Omnibus Rule
  ▪ BA subject to civil and criminal penalties
  ▪ HHS to conduct periodic audits
  ▪ Penalties increased
  ▪ Civil money penalties distributed
  ▪ State attorney generals given authority
<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Penalty</th>
<th>Repeat Violations/YR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100‒$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000‒$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect—Corrected</td>
<td>$10,000‒$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect—Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
Business Associates–Omnibus Rule

- Subject to HIPAA security regulations
- Required to report breaches
- Subject to penalties
- Agreements with BAs must be amended
- Business Associates and the Omnibus Rule
Key Changes…

- Business Associate (BA) definition expanded
- Liability and obligations of BA expanded
- Marketing, fundraising, sale of PHI
- Change in Notice of Privacy Practices
- Patient right to restrict disclosure to health plan if visit is paid in cash and patient requests a restriction
- Enhanced rights for individuals to receive electronic copies of PHI
Key Changes…(continued)

- Health plans prohibited from disclosing genetic information for underwriting purposes
- Modify individual authorization and requirements to facilitate research and disclosure of child immunization proof to schools
- Enable access to decedent information by family members or others
- Increased penalties for noncompliance
Privacy Notice Changes…

- Inclusion of use/disclosure of PHI for marketing, selling PHI, disclosure of psychotherapy notes
- Inclusion of use/disclosure of PHI for fundraising, and note patients’ right to opt out of such use and disclosure
- Covered Entity health plans intending to use PHI for underwriting purposes must give notice and advise individuals that Covered Entity is prohibited from using genetic information for underwriting purposes
Privacy Notice Changes… (continued)

• Covered Entity has legal obligation to notify individuals if their PHI is affected by security breach

• Inclusion of description of individual’s right to request restrictions of disclosures to health plans for payment or healthcare operations regarding services for which individual has paid in full out of pocket
Notification of Material Change to Privacy Notice...

- HHS modified the method by which health plans are to notify participants of material changes to their notices of privacy practices.
- Health plans that post their notices on their Web sites may prominently post changes or their revised notices.
- In their next annual mailings, health plans must provide revised notices, or information about material changes and how to obtain revised notices.
Revised Breach Notification Rule

- Presumption of reportable breach
- “Compromised” information
- Omnibus Rule eliminates the “significant risk of harm” standard as the threshold for breach notification
Revised Breach Notification Rule... (continued)

- New standard presumes reportable breach occurred **unless** Covered Entity or Business Associate determines a **low probability** PHI was compromised by unauthorized use or disclosure.
- Covered Entities and Business Associates must revise breach notice policies and procedures to reflect new breach analysis standard.
HIPAA Scenario #3

How does the HIPAA Omnibus Rule affect data breaches?

1. Organizations will be fined every time they report a breach.
2. Health organizations will have to start at the top to change their culture and ensure that they clearly document their security policies and methods for responding to breaches.
3. Providers will continue to use the interim rule as a harm threshold to assess whether they’re subject to penalties in the event of a data breach.
Marketing

- Omnibus Rule imposes stricter limitations on marketing communications made in exchange for financial remuneration
- Written communications promoting purchase or use of third party products or services, require prior individual authorization if Covered Entity receives financial remuneration in exchange for sending the communication
HIPAA Scenario #4

Which groups are not considered covered entities under the HIPAA Omnibus Rule?

a. The US Postal Service, United Parcel Service, delivery truck line operators, and certain internet service providers.

b. Business associates and their subcontractors.

c. The 19,000 covered entities and their thousands of BAs.

d. Patient safety organizations, health information organizations, e-prescribing gateways, and personal health records vendors.
Fundraising...

- Omnibus Rule provides limited set of circumstances for Covered Entity to use and disclose certain PHI for fundraising without an authorization.
- Covered Entities must provide an individual with clear and conspicuous opportunity to opt-out of receiving future fundraising communications.
Increased Patient Rights

- Patient access
- Who can receive?
- Can patient restrict access?
- Notice of privacy practice for patients
Action Items

- Revise policies and procedures
- Revise policy and security policies
- Revise privacy notice
- Revise breach notification requirements
- Revise Business Associates contracts/agreements
- Encryption
- Staff training
What Actions Are Required?

• Revise Business Associate Agreements
• Evaluate existing contractor arrangements to determine whether modifications or new agreement provisions are necessary, including to existing Business Associate Agreements
• Revise HIPAA Policies and Procedures, including modifications to address response to potential breaches involving unsecured PHI
Compliance Strategies under HIPAA Omnibus

- Confirm that PHI meets National Institute of Standards and Technology (NIST) standards
- Staff education and periodic review
- Consult with your professional liability insurance carrier
- Identify all current business associates (BA)
- Gather all existing BA agreements
- Identify if any BA is missing an agreement
References and Resources


• Federal Register, October 30, 2009. HIPAA Administrative Simplification: Enforcement


• http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

• http://www.thedoctors.com/KnowledgeCenter/PatientSafety/InformedConsent/index.htm?q=1&icf=1&s specialty=48
Mission Statement

Our Mission is to Advance, Protect, and Reward the Practice of Good Medicine

For additional Patient Safety information, please visit our web site at www.thedoctors.com and click on Patient Safety