HIPAA Training for the Medical Office
Disclaimer

The information and any commentary contained in these training materials is for informational purposes only. The information and commentary in these materials do not – and are not intended to constitute advice (legal or otherwise) to any person or entity on a specific situation or matter. You should always consult a qualified professional for advice regarding and tailored to your specific circumstances.
Today’s Agenda

- HIPAA History
- Enforcement & Penalties
- HIPAA Privacy
- HIPAA Security
- Breach Notification
- Resources
HIPAA History
HIPAA History

- Health Insurance Portability and Accountability Act (HIPAA)
  - Privacy, April 14, 2003
  - Security, April 20, 2005

- Health Information Technology for Economic and Clinical Health (HITECH) Act
  - Amended HIPAA in 2009
  - Enhanced enforcement
  - Breach notification, September 23, 2009

- Omnibus HIPAA Final Rule
  - Implements amendments to HIPAA included in the HITECH Act
  - Compliance required September 23, 2013
Enforcement and Penalties
Enforcement

- The Department of Health and Human Services (HHS), Office of Civil Rights (OCR) is responsible for enforcement.
- Any person may be prosecuted, including unauthorized individuals who obtain or disclose PHI.
- Civil money penalties to be shared with harmed individuals.
- HHS Secretary is required to perform periodic compliance audits.
- State Attorneys General may bring civil actions on behalf of residents damaged by violations.
Civil Monetary Penalties

- Did Not Know: $100 - $50,000
- Reasonable Cause: $1,000 - $50,000
- Willful Neglect Not Corrected: $50,000
- Willful Neglect Corrected: $10,000 - $50,000

Up to $1.5 million per violation, per year
Criminal Penalties

Enforced by Department of Justice

- **Being curious / gossiping**
  - $50k, 1 year jail

- **Lying to obtain information**
  - $100k, 5 years jail

- **Personal gain / malicious harm**
  - $250k, 10 years jail
The Basics of HIPAA Privacy
Required to Comply with HIPAA

- **Covered Entities (CE)**
  - Healthcare providers that conduct “certain transactions” in electronic form, such as
    - Healthcare claims
    - Eligibility status
    - Electronic remittance advices
- **Health plans**
- **Healthcare clearinghouses**
- **Business associates (BA) of covered entities**
Business Associates (BA)

- Performs activities/services, on behalf of a covered entity, that involve the use or disclosure of Protected Health Information
- Covered entities must have Business Associate Agreement (BAA) in place with all Business Associates
- Sample BAA language available at SVMIC.com
What Information is Protected?

**HIPAA Privacy**

- Protects “individually identifiable health information” in any form
  - Electronic
  - Paper
  - Oral Communication

**Protected Health Information (PHI)**

- Past, present or future healthcare or payment for healthcare provided to an individual
  - Includes demographic information
Individual Identifiers

1. Name
2. Any address specification (street, city, county, zip code, etc.)
3. All dates including birthdate, admission/discharge date, etc.
4. Telephone number
5. Fax number
6. Email address
7. Social security number
8. Medical record number
9. Health plan beneficiary number
10. Account number maintained by healthcare provider
11. Driver’s license number
12. License plate number
13. Medical device identifier/serial number
14. Web address
15. IP address
16. Fingerprints or other biometric identifier
17. Full face photo
18. Any other unique identifying number, characteristic or code
Minimum Necessary

- Health care providers are required to take reasonable steps to limit the use and disclosure of PHI to the Minimum Necessary to accomplish the intended purpose of the disclosure
  - Sign-in sheet
    - More detailed personal patient information should be collected discretely
    - Patient name, time of appointment, doctor being seen

- Policies and procedures must be in place that restrict access and uses of PHI based on specific roles of workforce
  - Access to PHI should be restricted to ONLY information required to do that specific job
Permitted Uses and Disclosures

- Not required to obtain the patient’s consent to disclose PHI for purposes of *treatment, payment or healthcare operations (TPO)*

- Examples of TPO uses and disclosures
  - Sending medical records to another physician who is treating your patient
  - Faxing clinic notes to a healthcare payer for reimbursement
  - Conducting an internal chart audit
Authorized Uses and Disclosures

Required to obtain a patient’s authorization to use or disclose PHI for non-TPO purposes

- Requests from attorneys
- Completion of disability forms
- Research
- Marketing
- Sale of PHI
Incidental vs. Unlawful Disclosures

- Incidental disclosures of PHI as a result of permitted disclosures are not violations of HIPAA

Examples of incidental disclosures
- Calling a patient back by their first and last name
- A patient overhears a discussion for the order of a test for another patient while on the way to the exam room

If you are aware of issues, consider solutions

Examples of unlawful uses and disclosures
- Accessing a patient’s information out of curiosity
- Discussing patient information outside the clinic setting
Communicating with Others Involved in the Patient’s Care

HIPAA Privacy Rule Disclosures to a Patient’s Family, Friends, or Others Involved in the Patient’s Care or Payment for Care

- If the patient is present and has the capacity to make health care decisions the provider may disclose relevant information if the provider does one of the following:
  1. Obtains the patient’s agreement
  2. Gives the patient an opportunity to object and the patient does not object, or
  3. Decides from the circumstances, based on professional judgment, that the patient does not object

- If the patient is not present or is incapacitated the provider may disclose relevant information if, based on professional judgment, the disclosure is in the patient’s best interest.

- For more information see: A Health Care Provider’s Guide to the HIPAA Privacy Rule: Communicating with a Patient’s Family, Friends, or Other’s Involved in the Patient’s Care http://www.hhs.gov/sites/default/files/provider_ffg.pdf
Notice of Privacy Practices

◆ Notice should have been updated in 2013
  – Sample available at: https://www.healthit.gov/providers-professionals/model-notices-privacy-practices

◆ Health care providers must do ALL of the following:
  – Provide a copy of the Notice and obtain acknowledgment (new patients only)
  – Post in prominent location
  – Post on website
  – Make the Notice available upon request
Patient Rights

- Receive Notice of Privacy Practices
- Request confidential communications
- Request amendment of PHI
- Receive an accounting of disclosures
Patient Rights: Access to PHI

Access PHI Electronically
- Patient portals, CDs, USB drives, email
- Form and format of PHI determined by patient request

PHI Transmitted to a Third Party
- Request must be in writing
  - Designated person to receive the information
  - Where the information should be sent
- Patient’s signature

More Information: HHS Guidance to Patient Access:
http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
Parent Access to Minor Child’s PHI

- Typically, both parents have the authority to access and control their minor child’s PHI, unless a court order forbids access.

- EXCEPTION: When a minor can obtain a particular health service without parental consent under state or other applicable law, it is the minor, not the parent, who may exercise the privacy rights afforded to patients under this regulation.

- The Privacy Rule defers to state laws that require, permit or prohibit the covered entity to disclose a minor’s PHI to a parent.

- Check specific state law for further exception information.
Patient Rights: Right to Request Restriction

- Patient may request a restriction on uses and disclosures for treatment, payment or healthcare operations
  - Health care provider may decline if request is unreasonable or would affect the patient’s care

- Health Plan Restriction
  - If a patient pays out-of-pocket, in full, for a particular service they can ask you not to disclosure this information to their health plan
    - **Health care providers must agree to this restriction**, unless the disclosure is required by law
The Basics of HIPAA Security
Focus of the Security Rule

- Electronic PHI (e-PHI)
- Health care providers must protect the confidentiality, integrity, and availability of all e-PHI that is created, received, maintained, or transmitted
- Required Risk Analysis and the establishment of administrative, physical and technical safeguards
Communicating PHI Electronically

- Email/text messaging is not specifically prohibited by HIPAA.
- However, HIPAA requires appropriate physical, administrative and technical safeguards for all PHI.
- Any device used to store, transmit or receive PHI must be included in Security Risk Analysis (laptops, smartphones, tablets, USBs).
Email

- Include email in Security Risk Analysis
- Encrypted PHI = Secure PHI
- Determine if email provider is a business associate. If so, have a business associate agreement in place.
- Email policy
SMS Texting

- HIPAA Issues
  - No authentication
  - No guarantee of password
  - Lost/stolen devices
  - Security risk analysis

- Secure messaging application
  - Business associate agreement

- Written texting policy
10 tips to protect and secure health information when using a mobile device.

1. Use a **password** or other **user authentication**
2. Install and enable **encryption**
3. Install and activate **remote wiping** or **remote disabling**
4. Do not install or use **file sharing applications**
5. Install and enable a **firewall**
6. Install **security software** and keep it up to date
7. **Research** mobile applications before downloading
8. Always keep your device **in your possession**
9. Use adequate security to send or receive health information over **public Wi-Fi networks**
10. **Delete** all stored health information before discarding the mobile device
Breach Notification
Breach Notification

- HITECH Act/Omnibus Rule
- Unauthorized access, use or disclosure of PHI considered a Breach unless “a low probability of the information being compromised” is proven
  - Faxing records to unauthorized individual
  - Providing copies of patient information to the wrong patient
  - Lab results mailed to the wrong patient
- Required risk assessment
- More information about the Breach Notification Rule
  - [www.hhs.gov/hipaa/for-professionals/breach-notification/index.html](http://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html)
Notification Process

◆ Patient Notification
  – Written notice no later than 60 days after discovery
  – Must be sent by first class mail or email, if requested

◆ Notification to Government
  – Annual reporting to HHS for breaches less than 500
  – HHS within 60 days for 500+
  – Local media within 60 days for 500+ in one state

◆ Breaches of 500+ will be investigated by the Office of Civil Rights
**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:

### Breach Report Results

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtua Medical Group</td>
<td>NJ</td>
<td>Healthcare Provider</td>
<td>1654</td>
<td>03/11/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Network Server, Other</td>
</tr>
<tr>
<td>Karmanos Cancer Center</td>
<td>MI</td>
<td>Healthcare Provider</td>
<td>2008</td>
<td>03/10/2016</td>
<td>Loss</td>
<td>Other Portable Electronic Device</td>
</tr>
<tr>
<td>UHHS Geauga Medical Center</td>
<td>OH</td>
<td>Healthcare Provider</td>
<td>677</td>
<td>03/10/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>Illinois Valley Podiatry Group</td>
<td>IL</td>
<td>Healthcare Provider</td>
<td>26588</td>
<td>03/08/2016</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record, Network Server</td>
</tr>
<tr>
<td>Complete Family Foot Care</td>
<td>NE</td>
<td>Healthcare Provider</td>
<td>5083</td>
<td>03/07/2016</td>
<td>Hacking/IT Incident</td>
<td>Electronic Medical Record, Network Server</td>
</tr>
<tr>
<td>Premier Healthcare, LLC</td>
<td>IN</td>
<td>Healthcare Provider</td>
<td>205748</td>
<td>03/04/2016</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>21st Century Oncology</td>
<td>FL</td>
<td>Healthcare Provider</td>
<td>2213597</td>
<td>03/04/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>City of Hope</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>1024</td>
<td>03/04/2016</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>Centers Plan for Healthy Living</td>
<td>NY</td>
<td>Health Plan</td>
<td>6893</td>
<td>03/03/2016</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Walmart Stores, Inc.</td>
<td>AR</td>
<td>Healthcare Provider</td>
<td>4800</td>
<td>03/01/2016</td>
<td>Unauthorized Access/Disclosure</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>Eye Institute of Corpus Christi</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>43961</td>
<td>02/28/2016</td>
<td>Theft</td>
<td>Electronic Medical Record</td>
</tr>
<tr>
<td>Freeport Memorial Hospital</td>
<td>IL</td>
<td>Healthcare Provider</td>
<td>1349</td>
<td>02/28/2016</td>
<td>Theft</td>
<td>Other</td>
</tr>
<tr>
<td>Nintendo of America Inc.</td>
<td>WA</td>
<td>Health Plan</td>
<td>6248</td>
<td>02/28/2016</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>Valley Hope Association</td>
<td>KS</td>
<td>Healthcare Provider</td>
<td>52076</td>
<td>02/28/2016</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
</tbody>
</table>
Resources

- **SVMIC**  [www.svmic.com](http://www.svmic.com)
  - Sample forms
  - Webinars

- **Health and Human Services**  [www.hhs.gov/hipaa](http://www.hhs.gov/hipaa)
  - Privacy, Security, Breach Notification Rules
  - Guidance
  - Frequently asked questions

- **Health IT**  [www.HealthIT.gov](http://www.HealthIT.gov)
  - Mobile device protection
  - Privacy/Security resources
  - EHR Implementation and Security Risk Analysis tools

- Additional resources
Resources: Documents

- Sample Business Associate Agreement
- Sample Communicating with Patient’s Family and Friends
- Sample Request for Electronic Copy of PHI
- Sample Request to Transmit PHI to a 3rd Party
- Sample Request to Restrict Disclosure of PHI to a Health Plan
- Sample Breach Notification Policy
- Sample Breach Notification Letter
Thank you!