This training is designed to provide a comprehensive look at HIPAA.

To ensure the privacy of Protected Health Information (PHI), avoid potential civil and criminal penalties and aid preparedness for potential audits from the Department of Health and Human Services (HHS), it is extremely important that all VCU Dental Care, LLC and School of Dentistry (SoD) faculty, staff, and students have a solid understanding of HIPAA and its requirements.
Section I
Introduction to HIPAA

- What is HIPAA?
- What is Portability?
- What is Accountability?
- HIPAA Legislation Timeline
- How is HIPAA Enforced?
- Why Do We Need HIPAA?
- Who Must Abide by HIPAA?
- What is a Covered Entity?
- How Does HIPAA Affect Me?
What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law passed by Congress in 1996. It was passed as an attempt at progressive healthcare reform.

HIPAA’s intent is to reform the healthcare industry by reducing costs, simplifying administrative processes and burdens, improving the portability and accountability of health insurance coverage, and improving the privacy and security of our patients’ information.

Many experts consider HIPAA to be the most significant US healthcare legislation since Medicare was passed in 1965.
What is Portability?

The HIPAA portability provision is designed to improve the portability of health coverage for people who are changing jobs and to make it easier to add family members to an employees’ coverage.

It also placed limits on group health plans’ exclusion period and restrictions for coverage of pre-existing conditions.
The HIPAA accountability provision implemented the Administrative Simplification Rules. The purpose of the Administrative Simplification Rules was to save money and increase efficiency of the health care system by creating standards for electronic transactions.

This led to concerns regarding the privacy and security of individual health information. Because of these concerns, the Department of Health and Human Services (HHS) developed additional requirements that addressed:

- Privacy;
- Security;
- Transactions and Code Sets; and
- Unique Identifiers.
HIPAA Legislation Timeline

HIPAA Timeline

After the original passing of the HIPAA regulations in 1996, HIPAA updates were included in the federal stimulus bill known as the American Recovery and Reinvestment Act of 2009 ("ARRA"). Those updates are referred to as the Health Information Technology for Economic and Clinical Health Act or ("HITECH") Act.

Anticipating the massive expansion in the exchange of electronic protected health information (ePHI), the HITECH Act expanded the scope of privacy and security protections available under HIPAA in addition to allowing for more enforcement and increased penalties for non-compliance.

The Omnibus rule essentially incorporated the HITECH Act provisions back into the official HIPAA regulations and also provided more detailed guidance.

© Copyright 2001-2019 HIPAATraining.com, All Rights Reserved.
Why Do We Need HIPAA?

- **It's the Law!** It is required by the Department of Health and Human Services (HHS).
- **It enables us to build trust** between our Faculty, Students, Providers, Business Associates, and Patients.
- **HIPAA protects our reputation.**
Covered Entities are Health plans, healthcare clearinghouses, and healthcare providers who electronically transmit health information in electronic format in performance of a Covered Function.

- Healthcare professional (example: hospital or physician)
- Healthcare plan (example: managed care program)
- Healthcare clearinghouse (example: third-party billing center)
If you currently see, use or share an individual’s PHI as part of your official daily job functions or school assignments, you are required to protect the privacy of patients and their PHI. This includes when you are:

- At a **Workstation**
- In **Clinic**;
- In **Class**; OR
- Signed in to **ANY Information System** that stores, processes or transmits PHI.
Section II
All About PHI

- What is Protected Health Information?
- What is Considered Individually Identifiable Information?
- What Are the 18 PHI Identifiers?
- What PHI/ePHI is Protected by HIPAA?
- What is HIPAA Used For?
- Examples of PHI
- Examples of ePHI
HIPAA revolves around protecting sensitive health information.

The official term for this sensitive information for HIPAA purposes is known as Protected Health Information (PHI).

PHI can be electronic or non-electronic. When PHI is in its electronic form it is referred to as Electronic Protected Health Information (ePHI).

PHI is any individually identifiable health information.
What is Considered Individually Identifiable Information?

- There are 18 HIPAA Identifiers that are considered individually identifiable information.

- This information can be used to identify, contact, or locate a single person or can be used with other sources to identify a single individual.

- All of this information must be De-Identified PRIOR TO providing it to an unauthorized individual or someone without a need-to-know.
What Are the 18 PHI Identifiers?

Here’s the list of PHI identifiers:

1. Names
2. All geographical subdivisions smaller than a State
3. All elements of dates (except year) related to individual
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including fingerprints
17. Full face photographic images
18. Any other unique identifying number
HIPAA protects PHI or ePHI regardless of the form in which it is maintained that is:

- Transmitted in paper, electronic, photographs/radiographs and/or verbal communications;
- Created or received by a health care provider, health plan, or health care clearinghouse; or
- Relating to the past, present, or future physical or mental health or condition of an individual.
Here are some examples of PHI that you may encounter:

- Faxes
- Health Care Invoices
- Patient Receipts
- Sign In Logs at Registration
- Mail Containing PHI
- Recommendation for Admission Forms
- Health Care Insurance/Claim Forms
- Print Outs of PHI from any electronic health records system

45 CFR 403.812
Examples of ePHI

— ePHI can be any PHI electronically accessed in ANY Information System.

— Here are some examples of PHI:
  - Encounter/visit documentation
  - Lab results
  - Appointment dates/times
  - Invoices
  - Radiology films and reports
  - History
Section III
Privacy Rule and Security Rule

- HIPAA Privacy Rule
- HIPAA Security Rule
- HIPAA Privacy Rule vs Security Rule
The HIPAA Privacy Rule:

- Protects the privacy of PHI by establishing conditions for its use and disclosure for Health Plans, Health Care Clearing Houses, and Health Care Providers.

- Allows for the secure flow of PHI needed to provide health information needed to provide and promote high quality health care.
The HIPAA Security Rule ensures the confidence, integrity, and availability of PHI and ePHI that a covered entity creates, receives, maintains, or transmits.

**What is Confidentiality, Integrity, and Availability?**

**Confidentiality** – data or information is not made available or disclosed to unauthorized individuals.

**Integrity** – information has not been altered or destroyed in an unauthorized manner.

**Availability** – information is accessible and useable upon demand only by an authorized individual.
What's the difference between the **Privacy Rule** and **Security Rule**?

<table>
<thead>
<tr>
<th>Privacy Rule</th>
<th>Security Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WHAT</strong> is protected and <strong>WHO</strong> is permitted to use, disclose or access a patient's PHI</td>
<td><strong>HOW</strong> PHI or ePHI is properly safeguarded by using Technical, Administrative, and Physical standards</td>
</tr>
</tbody>
</table>

Examples: training, contracts, policies and procedures, etc.

Examples: firewalls, password policies, antivirus, encryption, etc.
Section IV
Permitted and Unpermitted Uses of PHI

- Permitted Uses and Disclosures of PHI
- Other Permitted Uses and Disclosures
Permitted Uses and Disclosures

45 CFR 164.502

Law Enforcement
Research
Public Health
Essential Government Functions
Judicial/Administrative Proceedings
Many health care providers and professionals have long made it a practice to ensure reasonable safeguards for individuals’ health information – for instance:

- By speaking quietly when discussing a patient’s condition with family members in a waiting room or other public area;

- By avoiding using patients’ names in public hallways and elevators, and posting signs to remind employees to protect patient confidentiality;

- By isolating or locking file cabinets or records rooms; or

- By providing additional security, such as passwords, on computers maintaining personal information.
Section V
Patient Rights

- Notice of Privacy Practices (NPP)
- Timely Access to See and Copy Records
- Right to Amend
- Right to Restrict Access
- Right to an Accounting of Disclosures
- Right to Revoke Authorization
Right to Restrict Access and Disclosure

— HIPAA has granted individuals the right to request restrictions regarding the use and disclosure of their PHI for treatment, payment, and healthcare operations.
Personal Representatives:
- The personal representative stands in the shoes of the individual and has the ability to act for the individual and exercise the individual’s rights.
- They essentially have the same rights as the patient and is legally authorized to make health care decisions for them.

Minors:
- Parents act as personal representatives to their children.
Section VI
HIPAA Privacy Requirements

- Training
- HIPAA Security Standards
- What is a Privacy Breach?
- Examples of a Privacy Breach
- How to File a HIPAA Privacy Breach
- How Can I Prevent A Breach?
- Penalties for HIPAA Privacy Violations
Training

— Workforce who handle PHI (i.e. Faculty, students, staff, affiliates, etc.) are required to complete training prior to being given access to an information system that contains PHI.

— Individuals who DO NOT complete the training and the attestation will have their accounts suspended until training and the attestation have been completed.
These standards assist us with maintaining HIPAA compliance.
A **Privacy Breach** means the acquisition, access, use, or disclosure of protected health information in a manner not permitted which compromises the security or privacy of the protected health information.

**Examples of Privacy Breaches:**

- Using social networks to talk about patients
- Looking at patient health information out of curiosity (without a legitimate business need to know)
- Discussing progress or prognosis in front of family members without the patient’s written consent
- Sending PHI to incorrect destinations
- Leaving printed patient health information unattended
- Using another person’s eID
The penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation with a maximum penalty of $1.5 million per year for violations of an identical provision.
Section VII
Making Sense of HIPAA Everyday

- Just a Little Peek
- Conversations in Public Places
- Leaving Workstations Unsecured
- Texting Patient Information
- Cloud Storage
- Proper Disposal Methods
- Approved Mobile Devices
- Keeping Passwords Confidential
- Safe Fax Use
- Phishing Scams
- Malicious Codes
- Antivirus Software
DON’T SNEAK A PEEK.

A “little peak” or “look” into a patient’s medical record is considered “snooping”. The same is true if you access files of research subjects without a legitimate reason.

This includes family members, friends, neighbors, etc.
ALWAYS SECURE YOUR PASSWORD(s).

Passwords …
- are unique to each user
- authenticate your presence on the system

So… take responsibility to keep it confidential!
- Never share your password with anyone else for any reason.
- Sharing passwords is a serious violation of and may result in disciplinary action.
- Password protect any mobile device that has PHI (i.e. VCU email).
Section VIII
Most Common HIPAA Violations & Breaches

- Recent Statistics for HIPAA Violations
- Most Common Causes of HIPAA Violations
- Recent Dental Office Violations
- Interesting HIPAA Facts
Recent Statistics for HIPAA Violations
Nationwide

- HIPAA violations are steadily growing for dental and health care practices.

- Policies and procedures provide us with guidance, but **YOU** must do everything you can to safeguard PHI and prevent it from getting into the wrong person’s hands.
Most Common Causes of HIPAA Violations
Nationwide

Most Common HIPAA Violations Causes

- Professional Hackers
- Incorrect Admin Procedures
- Insufficient IT Security Measures
- Employee Dishonesty
- Employee Accidental Disclosure
- Business Associate Disclosure
- Unauthorized access to records
- Unauthorized Access
- Lost or Stolen Devices
- Improper Disposal

Copyright © 2018 The HIPAA Guide
Interesting HIPAA Facts

HIPAA FACTS

- 1 in 7 healthcare organizations have still not appointed a HIPAA compliance officer
- 80% of healthcare organizations fail meaningful use audits
- 1 in 4 HIPAA breaches still not reported
- Unauthorized access to records accounts for 20% of HIPAA breaches
- 50% of healthcare organizations believe they would fail a HIPAA Audit
- Phishing and ransomware are the top hacker tactic
- Average cost per record is $363
- Ransomware for medical records is accelerating rapidly
- About 600 HIPAA Violations referred to DoJ
- Nearly 200 million patient records compromised since introduction of HIPAA

Copyright © 2018 The HIPAA Guide
Section IX

HIPAAASAFE Program

- HIPAAASAFE Compliance Program
- HIPAAASAFE Contact
Thank you for taking the 2019 HIPAA Privacy and Security Training!