UNIVERSITY of MARYLAND
SCHOOL OF DENTISTRY

HIPAA AWARENESS

HIPAA
Health Insurance Portability and Accountability Act

2020

Who am I?

Kent Buckingham, MS

Executive Director

Information Technology and Facilities Management

School of Dentistry

HIPAA and Security Officer

What's HIPAA?

- HIPAA stands for the "Health Insurance Portability and Accountability Act"
- It was passed by Congress in 1996
- Requests to gather public comment delayed HIPAA's starting date until 2003

What HIPAA Was Meant to Do?

- Allow people to move their health insurance coverage when they change jobs
- Streamline medical claims processing
- Reduce health care costs
- Ensure the privacy of medical records
- Establishes a single person in charge of privacy the HIPAA or Privacy Officer.

HIPAA's Original Three Important Parts

- The Privacy Regulation
- The Transaction and Code Sets Regulation
- The Security Regulation

HIPAA Privacy Regulation

- HIPAA protects many types of health information but it gives the greatest protection to personal health information
- What is health information?
- What makes health information “personal”?

What Is Health Information?

- Health Information is…
  - any information in the past, present, or future relating to the physical or mental health or condition of a person
  - Data about providing or paying for health care is also health information

- Examples of Health Information include:
  - Patient charts, X-rays, etc.
  - Doctor's appointment schedule
  - Medical bills, Worker's Compensation claims

What Makes Health Information Personal?

- Health information is “personal” if it can be associated with a person
- HIPAA lists 18 common pieces of personal information that make health information personal or individually identifiable
- These personal “identifiers” include a person’s name, address or phone number

But they also include…

- Birth date, admission or treatment dates
- Fax numbers
- E-mail addresses
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- License or certificate numbers, and…

As Well As …

- Vehicle license number
- Medical device serial number
- Web (URL) address
- IP address
- Biometric identifier (finger print, iris scan, etc.)
- Full-face photographic image
- Any other number or symbol, except as permitted by the regulations

Is All Personal Health Information Regulated?

- HIPAA regulations apply to personal health information only when:
  - This information is held by a Covered Entity, or
  - It is held by a Covered Entity's Business Associates
- Under these conditions, HIPAA defines personal health information to be Protected Health Information (PHI)

Privacy

- Establishes rights for patients to see or modify their own health information
- The Privacy Regulation defines who may see or use personal health data and what they can do with it
- Limits PHI use to the “minimum necessary”

Privacy (continued)

- Requires an authorization from a patient before his/her health information can be used for more than treatment, payment and normal health care operations.

- Restricts the use of e-mail for sending PHI to off-campus locations as well as to the Baltimore VA Hospital unless encrypted.

Basics of the HIPAA Privacy Rule

- UM personnel cannot see or use Protected Health Information unless it is required for the job.
- UM personnel can only see or use the minimum amount of Protected Health Information that is necessary for a task
- UM personnel who see or use Protected Health Information in violation of HIPAA have violated federal law, are subject to fines, jail, and UM disciplinary action which may include termination

Failure to keep PHI confidential can lead to…

- Identity theft
- Incorrect or incomplete treatment decisions
- Lost patient confidence & loyalty
- Adverse public relations
- Legal fees associated with defending lawsuits
- Monetary damages and penalties

Physical and Technical Safeguards of PHI

HIPAA requires that we put in place safeguards, such as:

- Restricting patient and visitor access to non-patient care areas
- Locking offices and controlling access to office keys
- Safeguarding medical records and assuring proper disposal
- Limiting ability to view computer screens
- Using screen savers that automatically lock or log off after periods of inactivity
- Restricting access to electronic patient information
- Safeguarding ePHI sent in e-mails, stored on PDAs, laptop computers and on cellular phones
- Secure destruction of PHI data.

University of Maryland Baltimore HIPAA/Privacy Officers

University of Maryland Baltimore

- Privacy Officer
  Dr. Peter Murray
  410-706-2461

Covered Entities:

School of Dentistry

- Privacy and Security Officer
  Mr. Kent Buckingham, MS
  410-706-0343

School of Medicine

- HIPAA Privacy Officer
  Stanford Stass, M.D.,
  Professor and Chair, Department of Pathology
  410-706-7070
- HIPAA Security Officer
  Sharon Bowser, MBA
  Associate Dean and Chief Information Officer (CIO)
  410-706-0412

Privacy - In Summary

- Keep Protected Health Information private and secure at all times
- Make sure only UM Personnel who need to use Protected Health Information see it or use it
- Use only the minimum amount of Protected Health Information necessary to accomplish the task
- Read and understand UM Privacy policies and procedures
- Know your Privacy Official
- Consult your Privacy Official with any questions you have about privacy or Protected Health Information

Transaction and Code Sets

- The Transaction and Code Sets Regulation standardizes the electronic format and content of medical billing

- It affects those who prepare, send or receive claims or who verify eligibility for delivery of health care services

Security

- The Security Regulation sets standards for computers and networks that store or transmit personal health information
- Computer security helps to make the HIPAA Privacy Regulation work

Reasonable Security Measures for Protected Health Information

- Use and do not share computer passwords
- Lock doors, lock file cabinets, and limit access to workspace where health information is used or stored
- Limit access to printers and faxes where health information is printed
- Limit access to health information to only those who need it for a specific task

Reasonable Security Measures for Protected Health Information Continued

- Encrypt all ePHI data transmitted and at rest.
- Shred or otherwise properly dispose of health information trash.
- Remove terminated employee access immediately.
- Follow the University's privacy policies and procedures.

UNIVERSITY of MARYLAND
SCHOOL OF DENTISTRY

HIPAA's Timetable

Regulation	*Date*	*Focus*
HIPAA	1996	Electronic communications
Security Rule	2003	Securing Electronic PHI
HiTech Act	2009	Establishes penalty structure
HIPAA Omnibus rule	2013	Privacy details

How HIPAA Affects You

- The University of Maryland Baltimore considers itself a hybrid entity. Since it is home to a large number of health care activities and two covered entities:
  - School of Dentistry
  - School of Medicine
- Information about people's health is everywhere on this campus
- HIPAA protects this information by regulating how others are allowed to see and use it.

What is a Covered Entity?

- A Covered Entity (CE) is a health care provider, a health care plan or a clearinghouse
- Employees of CEs are also regulated by HIPAA
- UMB must comply with HIPAA regulations because schools, departments and other groups on its campus engage in clinical activities that collect and use PHI

UNIVERSITY of MARYLAND
SCHOOL OF DENTISTRY

Covered Entities:

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
This includes providers such as: •Doctors •Clinics •Psychologists •Dentists •Chiropractors •Nursing Homes •Pharmacies ...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.	This includes: •Health insurance companies •HMOs •Company health plans •Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

What is a Business Associate?

- A Business Associate (BA) is an organization that sends, receives, uses or works with PHI on behalf of a Covered Entity
- Examples of BAs include collection agencies, transcriptionists, contractors working with PHI, etc.
- BAs and their employees must also comply with HIPAA

How do I establish a Business Associate?

- A Covered Entity will enter into Business Associate (BA) agreement with any company that will have access to PHI data. Providers, labs and insurance companies are excluded. This agreement establishes the legal HIPAA relationship.

- BAs and their employees must also comply with HIPAA

HIPAA Regulations and UMB

Although you may not work for one of the covered entities:

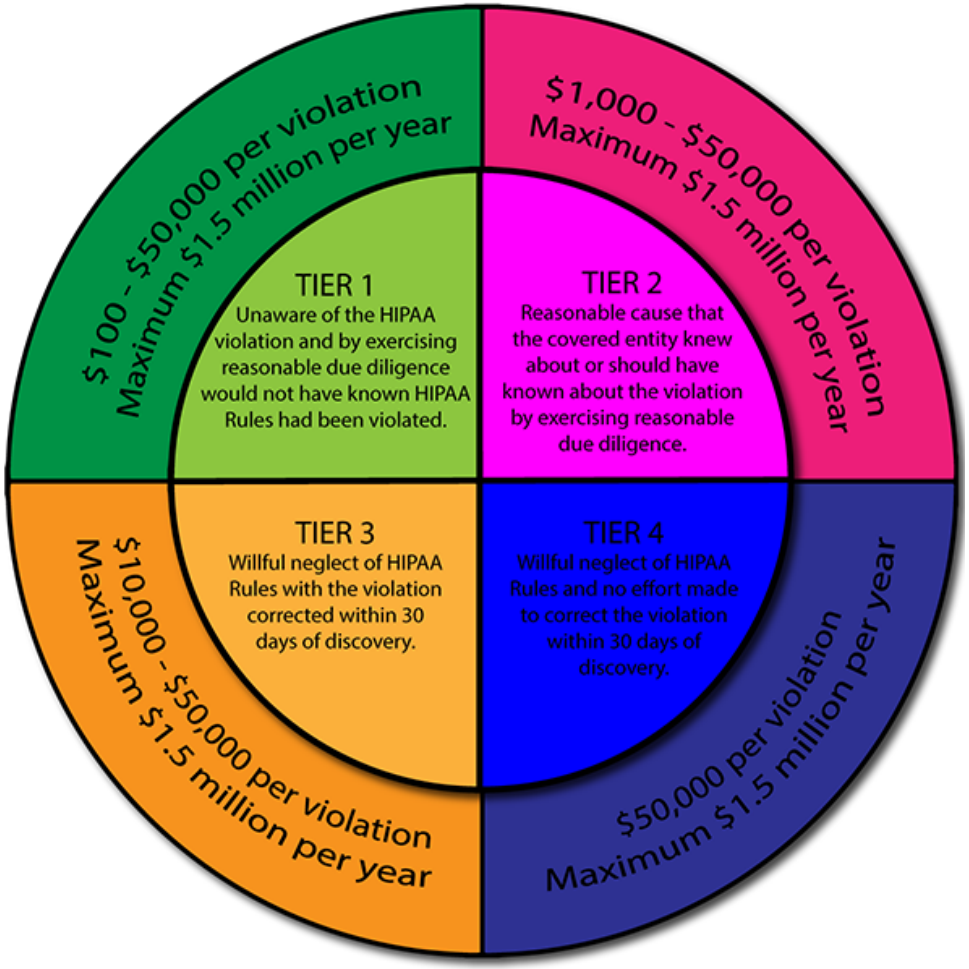
- All faculty, staff and students must protect any PHI that they may come into contact with.
- The university has strict privacy and security policies. The violation of these policies could lead to disciplinary actions and termination.

HITECH Act 2009

Health Information Technology for Economic and Clinical Health Act-**HITECH Act**

- Created to expedite the use of electronic health records
- Tightened up HIPAA law to ensure Covered Entities and Business Associates were notifying individuals in the event their data was compromised.
- Tougher penalties for HIPAA compliance failures

HIPAA Violation Penalties



HIPAA JOURNAL

HIPAA Penalties

- General non-compliance
  - $100 per violation up to $25,000 per person per year
- Knowing disclosure of PHI
  - $50,000 and 1 year in prison
- Obtaining PHI under false pretenses
  - $100,000 and 5 years in prison
- Malicious harm or intent to sell PHI
  - $250,000 and 10 years in prison

HIPAA Omnibus Rule of 2013 Major Components

- Business associates' directly liable for compliance
- Strengthens limitations on using protected health information for marketing
- Prohibits sale of protected health information without authorization.
- Compound authorizations for research, and authorizing for future research studies
- Decedents and protected health information
- Disclosures to decedent's protected health information to family members and others involved in decedent's care

HIPAA Omnibus Rule of 2013 Major Components – Cont.

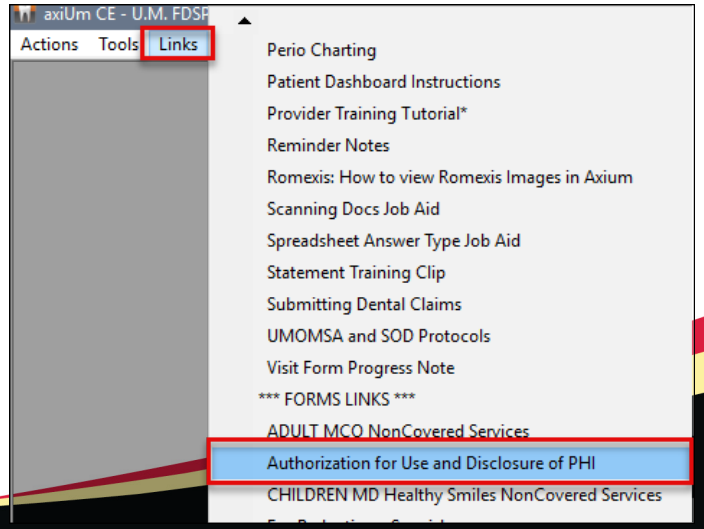
- Disclosure of immunization information to schools by covered entity.
- Fundraising and protected health information
- The need to update and distribute the notice of privacy practices
- Patients' right to restrict protected health information to a health plan for services not paid by health plan

HIPAA Omnibus Rule of 2013 Major Components – Cont.

- Access to protected health information in electronic formats
- Breach notification rule updates
- Genetic information is considered protected health information and not available for underwriting insurance
- Protects deceased individuals PHI for 50 years.

Patient Authorizations to Disclose PHI

You may not disclose PHI for any reason other than for treatment, payment, or healthcare operations and in some circumstances, to others involved in the patient's healthcare, without **written** patient authorization.



HIPAA Applies to Us

We each have a responsibility to respect and protect the privacy and security of our patient's health information.

It is important that we all understand and follow the HIPAA rules in order to:

- Learn to recognize PHI
- Keep PHI private and secure at all times.

HIPAA Privacy Rule applies to any form of Communication.

SPOKEN	PRINTED	COMPUTER SCREEN	FAX
EMAIL	PHOTOS	X-RAYS	TEXT

PHOTOS

Friendly HIPAA Reminder

- Please remember that ALL photos are to be taken with camera/devices offered by the school and transferred into the patient's chart immediately.
- Pictures are ***not*** to be taken/stored with personal cell phones.

Importance of Protecting Patient Health Information

Employees with access to patient data may use or disclose only on a “need to know” basis:

- Keep patient information confidential
- Access or use patient data only as required to perform your job
- **Do not discuss** patient information with others unless it is administratively or clinically necessary or patient authorized to do so
- **Do not use** any electronic media to copy or transmit information unless your are specifically authorized

Password Management is an Essential step to securing data

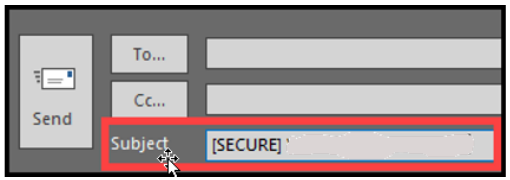
What should you consider when creating/managing a password?

- Make them **Strong**
- The password should use a mix of lower and upper case letters, symbols, and non-easily identifiable words, must be 9-14 characters ,
  Ex: sPo0kyH@LLoW3En
- Changed every 90 days.
- The password should be kept private at all times and **NOT shared with anyone**.

PHI in Email is a Security Risk

- Faculty and staff must use UMB email account for all emails, especially containing ePHI. You may not use a personal email account to send ePHI on or off campus unless encrypted.
- Email containing ePHI should be sent [SECURE] in subject line.
- You cannot put patient ePHI in subject line of an email.

EMAIL POLICY: USE ONLY FIRST ✓
INITIALLASTNAME@UMARYLAND.EDU



Certain Precautions may need to be taken when using email to avoid unintentional disclosures:

- Check email address for accuracy
- Send an email alert to patient for address confirmation prior to sending the message
- Limit the amount of information disclosed in email

The Negatives of Texting in Healthcare

- Reside on device and not deleted
- Very easily accessed
- Not typically monitored
- Can be compromised in transmission relatively easy
- Phone carrier can store data information
- Not secure
- Uncertainty the message is received by intended recipient

Google Voice Text is not a Secure method of texting

Backline offers a secure messaging solution for healthcare that meets all HIPAA, HiTECH ACT and Joint Commission requirements

A patient has the right under the Privacy Rule to request alternative means or locations to communicate. This rule does allow health care providers to communicate electronically provided they apply reasonable safeguards when doing so.

If a patient prefers to communicate by text, please use the Backline resource provided to you.

Cyber Attacks are the #1 way health records are breached

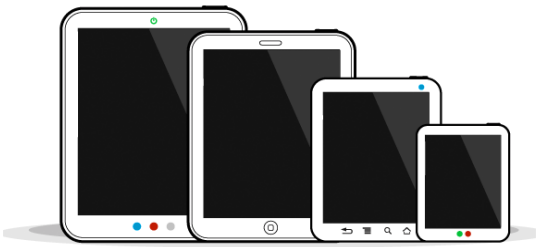
What Can You do to Help Secure our System?

- Please do not install software or games of any kind, without permission from OIT. These items can corrupt our system and comprise our data
- Do not open any emails from untrusted sources
- Lock your laptop or computer when you walk away

Rules for Mobile Devices

We REQUIRE that you REGISTER Devices if they are being used for Patient Health information.

- Devices can be registered by email, send to SODHelp@umaryland.edu or stop by the OIT desk to register device
- Please provide serial number /type/phone #
- Must be Password protected
- Mobile Devices must be Encrypted
- Must *not* be used for storage of confidential information



NO SOCIAL MEDIA POSTINGS OF PATIENTS

Safeguard your Computer's Information

BEFORE YOU WALK AWAY……

LOCK YOUR DISPLAY

- ✓ Press the Windows logo key and the ‘L’ key at the same time. The computer will automatically lock.

OR….

- ✓ Press the Ctrl, Alt, and Delete keys at the same time. Then click on ‘Lock.’

Compliance Manager Audits

- **Periodically walks through clinic looking for privacy educational opportunities.**
  - First infraction receives a verbal warning.
  - Second infraction receives a written warning.
  - Third infraction must meet with Privacy Officer.

  *If infraction is severe then must meet with Privacy Officer.

Regulations

- HIPAA protects PHI by defining Covered Entities and assigning the Office of Civil Rights as the enforcement agency.
- There are many federal and state laws and governing bodies that protect confidential data.
- Employers like the university have policies that protect confidential data.

Don’t get burned!

- Although you may not be a covered entity.
- You could lose your job or even go to jail for not protecting PHI.

Helpful Websites

FPI Compliance Website

http://intranet.upi.umaryland.edu/compliance/

School of Medicine HIPAA Website

http://medschool.umaryland.edu/HIPAA/

U.S. Dept. of Health & Human Services, Health Information Privacy

http://www.hhs.gov/ocr/privacy/

- **UPI Compliance Website**
  http://intranet.upi.umaryland.edu/compliance

- **Center for Medicare and Medicaid Services**
  http://www.cms.hhs.gov/hipaa/hipaa2/

- **HIPAAdvisory**
  http://www.hipaadvisory.com/

- **US-CERT Computer Security Tips**
  http://www.us-cert.gov/cas/tips/index.html

Questions?