HIPAA:

What You Need to Know

Anne-Tyler Morgan

McBRAYER

Overview

- What is HIPAA and why is it important?
- What is the HIPAA principle and to whom does it apply?
- What does HIPAA mean operationally?
- What is Protected Health Information?
- What do you have to know?
- Protecting Patient Privacy.
- Safe Information Practices and what you can do.
- When has a breach occurred?
- Examples of Breaches.
- Questions and Answers.

HIPAA
Health Insurance Portability and Accountability Act

McBRAYER

What is HIPAA?

- Health Insurance Portability and Accountability Act (HIPAA)
  - Privacy Rule, Security Rule
  - Requires "minimum necessary" use and disclosure
  - Specifies patient's right to approve the access and use of protected health information (PHI)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Amended HIPAA in 2009
  - Breach notification requirements
  - Outlines patient's right to request copies of electronic health record in electronic format
- In general, covered entities such as health plans, health care clearinghouses, and health care providers which conduct certain financial and administrative transactions electronically must comply with the HIPAA regulation.

McBRAYER

What is the HIPAA Principle?

The concept of HIPAA's Privacy and Security Regulations is simple:

KEEP INDIVIDUALS' HEALTH INFORMATION SECURELY CONFIDENTIAL

McBRAYER

Why is HIPAA Important?

- HIPAA calls for severe civil and criminal penalties for noncompliance.
- There are potential penalties for non-compliance which apply to you as an individual and as an institution:

Violation Category	Each Violation	Total CMP for Violations of an Identical Provision in a Calendar Year
Unknowing	$100 – $50,000	$1,500,000
Reasonable Cause	$1,000 – $50,000	$1,500,000
Willful Neglect – Corrected	$10,000 – $50,000	$1,500,000
Willful Neglect – Not Corrected	At least $50,000	$1,500,000

Criminal Liability

- In June 2005, the U.S. Department of Justice (DOJ) clarified who can be held criminally liable under HIPAA.
  - Covered entities and specified individuals, whom "knowingly" obtain or disclose individually identifiable health information in violation of the Administrative Simplification Regulations face a fine of up to $50,000, as well as **imprisonment up to one year.**
  - Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to **five years in prison**.
  - Offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and **imprisonment for up to ten years**.

McBRAYER

To Whom Does HIPAA Apply?

- "Covered Entities"
  Health Plans, Health Clearinghouses and Health Care Providers
- "Business Associates" of covered entities
  Vendors, Consultants, Contracted service providers, Others

McBRAYER

What Does HIPAA Mean Operationally?

It's all about Protected Health Information (PHI).

HIPAA requires:

- **procedural safeguards**
- **physical safeguards and**
- **electronic safeguards**

to protect the privacy and confidentiality of PHI.

McBRAYER

What is PHI?

- Protected Health Information
- Information, including demographic information which relates to:
  - The patient's past, present, or future physical or mental health
  - The provision of health care to the patient
  - The past, present, or future payment for the provision of health care to the patient
- PHI identifies the patient or can be used to identify the patient
- Can be in any form: written, spoken, or electronic (including video, photographs and x-rays)

McBRAYER

Elements of a Record That Can be Used to Identify a Patient

- Name
- Address
- Dates (birthdate, admission date, discharge date, etc.)
- Telephone number
- Fax number
- Email address
- Social security number
- Medical record number
- Health plan member ID
- Full face photos
- Etc.

McBRAYER

The Rules apply when you VIEW, USE, or SHARE PHI

- As health care workers, you see and hear confidential information every day on the job.
- You get so accustomed to being around PHI that it is easy to forget how important it is to keep it private.
- Privacy and confidentiality is a basic right in our society.
- **Safeguarding that right is your <u>ethical and legal obligation</u>.**

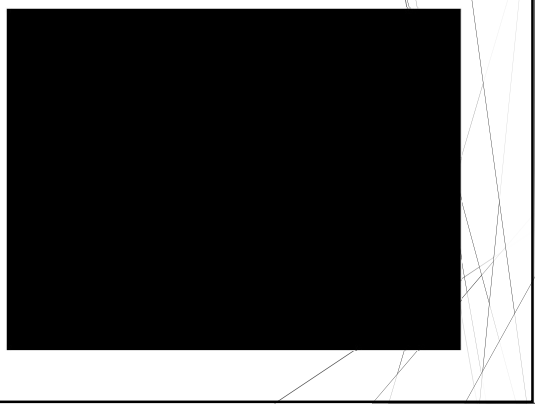
McBRAYER

Use vs. Disclose

- Use = Information passing within "the family"
- Disclose = Information passing outside "the family"

"Are you here with Leon Fineman, the 57 year old that came in for a triple hemorrhoidectomy? He's doing fine."

McBRAYER



Allowable Use & Disclosure

- Treatment
  - Except for:
  - Psychotherapy treatment, HIV tests, and substance abuse information, providers may use and disclose PHI for treatment and patient care
- Payment
  - Minimum necessary standards apply
  - Example: Billing clerk may need to know lab test was performed but not the test results
- Operations
  - Example: Licensing board requests copy of records pursuant to investigation
  - Minimum necessary standards apply

McBRAYER

REMEMBER…

- Use PHI **only when necessary** to perform your job duties
  - "Need to Know Basis"
- Use only the **minimum necessary** to perform your job duties
- Follow facility policies and procedures for information confidentiality and security
- When violation occurs, report

McBRAYER

Hypothetical #1

Laura's Facebook page lists her occupation as a nurse at a rural practice that specializes in pain management. Using her personal computer after working hours, she makes this private post accessible only by her "friends" on her Facebook page:

"Today I got to meet Rock Star Jim! So excited!"

A comment to the post suggests that news reports that day state that Rock Star Jim's plane made an unscheduled landing in the area so that he could be treated for the flu.

In response, Laura replies,

"I know, but he came in to the clinic today because of his back."

Angela, also listed on Facebook as being a co-worker at the clinic, clicks "Like" on that comment.

- Has Laura violated HIPAA? Has Angela?

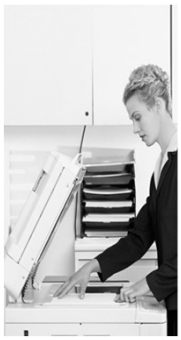
McBRAYER

Safe Information Practices

- Verbal exchanges
  - Confidential subjects discussed only in private settings (not in public places such as cafeterias, elevators, etc.)
  - Cautious use of cell phones
- Knowing where you left your paperwork
- Proper disposal of paper documents
- Locked and secure medical files
- Security of electronic PHI (e-PHI)
- Proper Computer Security

McBRAYER

Safe Information Practices



- Check printers, faxes, copier machines when you are done using them
- Ensure paper charts are returned to appropriate place at nursing station or designated file room
- Do not leave hard copies of PHI lying on your desk or work area. At the end of the day, lock it up.
- Seal envelopes well when mailing documents

McBRAYER

Disposal of Paper Documents

- Shred or destroy documents containing PHI before throwing away.
- Dispose of paper and other records with PHI in secured shredding bins. Recycling and trash bins are NOT secure.
- Obviously, shredding bins work best when papers are put INSIDE the bins! When papers are not left outside the bin, they are not secure from daily gossip, daily trash, the public.

McBRAYER

Computer Security

- Ensure your computer and data are physically secured by using lockdown cables, locked drawers, placement in a secured area
- Create strong password and do not share your username or password with ANYONE
- Log off your computer terminal before leaving
- Ensure information on computer screens is not visible to passerby
  - Use privacy screen if necessary
  - Lock your PC (Ctrl + Alt + Delete)
  - Use a password to start up or wake-up your computer
- Ensure your system has anti-virus and all necessary security patches and updates

McBRAYER

Data Security

There are tools for healthcare providers to use to provide greater data security:

- OCR recently published guidance that provides a crosswalk between HIPAA Security Rule and the NIST Cybersecurity Framework
- In May 2016, the White House touted the publication of the Data Security Policy Principles and Framework of the President's Precision Medicine Initiative, which also builds on the NIST Framework

McBRAYER

Texting Patient Orders?

- In 2011, the Joint Commission published a set of FAQs that prohibited physicians or licensed independent practitioners from texting orders for patients to hospitals or other healthcare settings.
- The concern was that the technology sending the messages was not sufficiently secure – there was an inability to verify the person sending the text as well as a failure of retention of the original message as validation of what is entered in the medical record.
- HOWEVER…

McBRAYER

Joint Commission and Texting Orders

May 2016 position reversal:

Licensed independent practitioners or other practitioners in accordance with professional standards of practice, law and regulation, and policies and procedures may text orders as long as a secure text messaging platform is used and the required components of an order are included.

Effective Immediately

McBRAYER

Avoiding HIPAA: Secure Texting Platform Safeguards

- Administrative Safeguards
  - Goal: prevent, detect, contain, and correct security violations
  - Risk analysis mechanisms, risk management plans, sanction policies for violators, and information system activity review procedure
- Physical Safeguards
  - Goal: Limit access
  - Contingency operations, facility security plans, access control, validation procedures, and records of maintenance
- Technical Safeguards
  - Goal: Digital specifications
  - Unique user identification, emergency access procedures, automatic logoffs, and encryption and decryption mechanisms

McBRAYER

Mobile Protection

- Use password or user authentication (ex: PINs)
- Catalogue physical inventory of devices
- Install and enable encryption
- Install and activate remote wiping and/or disabling
- Install and enable a firewall
- Install and enable security software
- Keep your security software up to date
- Use caution in downloading unverified mobile applications
- Disable and refrain from installing file sharing applications
- Wi-Fi network should be adequately secured
- Delete all stored PHI before disposal or reusing devices

Source: HealthIT.gov

McBRAYER

Telemedicine & HIPAA

- What is it?
  - E-Health, Telehealth, and Cybermedicine
  - Exchange of personal medical information from a physician over telecommunication technology.
- Positives
  - Expanded access to specialists
  - Chronic disease management
  - Homebound health care
  - Increase in overall community

McBRAYER

Telehealth & HIPAA: Risks

- Threat of Unauthorized Access
  - Hub site & Spoke site additional personnel
  - Access authorization protocols
  - Consent requirements
- Transmission Breaches
  - Live feeds
  - Taping sessions
  - Secure telecommunications line
  - Encryption

McBRAYER

Telemedicine & HIPAA: Best Practices

- Right to refuse
- Informed Consent
  - Alternatives to telemedicine
  - All personnel involved at both sites
- Consent and right to refuse video recording
- No limitation on subsequent service
- No difference in HIPAA requirements for PHI storage and usage

McBRAYER

Practice Safe Emailing

- Do not open, forward, or reply to suspicious emails
- Do not open suspicious email attachments or click-on unknown website addresses
- NEVER provide your username and password to an email request
- Delete spam and empty "Deleted Items" folder

McBRAYER

Faxes

- Faxes are the least controllable type of communication.
- ALWAYS use a cover sheet with a confidentiality statement and your location and phone number even on internal faxes.
- Never leave faxes sitting on fax machines unattended.
- It is critically important when faxing information:
  - to verify the sender has the correct fax number; and
  - that the fax machine is in a secure location, and/or the receiver is available immediately to receive the fax.

McBRAYER

What Can you Do? Be on Your Guard

- It is your responsibility for protecting patient privacy and confidentiality does not end with your work shift.
- Don't divulge any Patient information when in an informal atmosphere or social setting.
- If asked about a Patient, simply reply "I'm sorry, that information is confidential".
- Respect everyone as if they were your family member!

McBRAYER

(The person posting this had her car broken into)

McBRAYER

When has a Breach Occurred?

- A privacy breach can occur when information is:
  - Physically lost or stolen
    - Paper copies, films, tapes, electronic devices
    - Anytime, anywhere-- even while crossing the street, in the building, in your office
  - Misdirected to others outside of the facility
    - Verbal message sent or left on the wrong voicemail or sent to or left for the wrong person
    - Mislabeled mail
    - Misdirected email
    - Wrong fax number
    - Wrong phone number
    - Placed on internet, Facebook, Topix, Twitter
    - Not using secure email account

McBRAYER

Examples of Breaches

"Small" seemingly innocent activities that could lead to breaches:

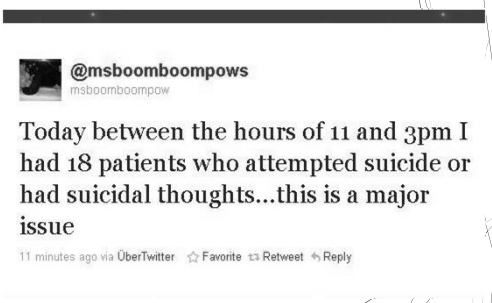
- An employee "checking" the record of a friend or family member, in order to see how they are doing.
- Leaving Patients' identifiable information on a computer screen that others can easily see.
- Neglecting to confirm accuracy of fax number before sending identifiable health information.
- Accessing the medical information regarding a Resident at the request of friends or family who are not entitled to that information.
- A high profile patient is admitted and you say to your colleague, guess who I just took care of? …Joe Celebrity

McBRAYER

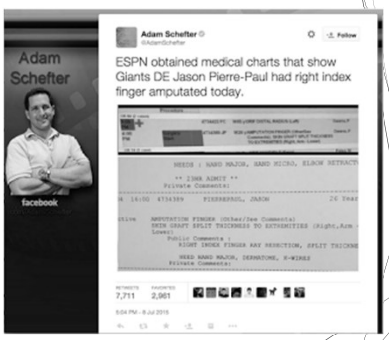
Examples of Breaches

- Leaving work at the end of the day and leaving patient information out on your desk rather than in a folder.
- Verbally communicating PHI to fellow co-worker with excessive volume (yelling down the hall).
- Discussing patient information on your cell phone in public areas.
- Not closing a privacy curtain when discussing patient information.
- Not logging off computer when you leave the area.

McBRAYER



McBRAYER



McBRAYER

How to Report Breaches

- Immediately report any known or suspected privacy breaches
  - Paper, conversations, suspected unauthorized access to, use or disclosure of PHI
- To Privacy Officer
- Anonymously by placing report in one of two secure drop boxes

McBRAYER

Hypothetical #2

Dr. Dan is a general practitioner in a Rural Health Clinic. One morning, two adults present with their 2-year old daughter, Natasha, who they say fell out of her bed and may have broken her leg. Dr. Dan immediately screens Natasha and gets her x-rayed and determines that her leg is indeed fractured. On a hunch, Dr. Dan pulls the medical records on Natasha and sees that just 2 months ago, Natasha was again brought to the clinic with suspicion of a sprained or broken wrist. Luckily, on that occasion, Natasha's wrist was just sprained. The medical record from that visit states that Natasha hurt her wrist when she fell out of bed.

Dr. Dan refers Natasha to an orthopedist, who sets Natasha's broken leg. Next, Dr. Dan calls local law enforcement and the state social services agency to report what he suspects to be child abuse, identifying Natasha and her parents by name.

- Has Dr. Dan violated HIPAA?

McBRAYER

Business Associate Agreements

- Business Associates ("BAs") are:
  - Exposed to potential federal criminal penalties for violation of HIPAA
  - Subject to regulatory jurisdiction of OCR and state attorneys general
  - Required to cooperate with OCR investigations of CE and Bas
  - Exposed to potential civil monetary penalties for violation of HIPAA
  - Can be exposed to private tort actions by individuals harmed by BA failure to comply with HIPAA
  - Examples:
    - Walgreens Indiana Verdict: $2 million

McBRAYER

Business Associate Agreements – Ten Items that MUST be Addressed

- Establish the permitted and required uses and disclosures of PHI by BA
- Provide that BA will not use or further disclose the information other than as permitted or required by the contract or as required by law
- Require the BA to implement appropriate safeguards to prevent unauthorized use or disclosure of the PHI, including compliance with the Security Rule for ePHI
- Require reporting to Covered Entity any improper use or disclosure, including breaches
- Require BA to make PHI available for access and amendment, and require information for accounting

[McBRAYER]

Business Associate Agreements – Ten Items that MUST be Addressed, cont'd

- Require Privacy Rule compliance, to the extent applicable
- Require BA to make books and records available to HHS
- Require return or destruction of PHI at termination, if feasible
- Require the BA to ensure that subcontractors agree to the same restrictions and conditions
- Authorize termination of the contract by CE if the BA violates a material term

[McBRAYER]

Business Associate Agreement Violations

- What do BA agreement violations look like?
  - A BA leases a copier and returns it without checking if the data has been removed
  - A hospital ships data tapes to an archiving service to be erased, and the archiving service loses a box of the tapes
  - An employee of a billing company for healthcare organizations has a laptop stolen that has billing data for patients

[McBRAYER]

HIPAA Enforcement

USDHHS Office of Civil Rights (OCR) May Investigate Compliance

- Based on complaint by any one – whistle blower, adversary, etc.
- Every notification of breach affecting 500 or more individuals is reviewed for potential investigation
- Notification of breach affecting fewer than 500 individuals may also trigger investigation

HIPAA Enforcement

OCR has also begun conducting audits of Covered Entities and Business Associates.

- **From 2011 to 2012, OCR conducted a pilot audit program (Phase 1) of Covered Entities to generally assess HIPAA compliance and gather information on how future audits can assist with compliance**
  - **115 Covered Entities were audited**
  - **Of 59 healthcare providers audited on the HIPAA Security Rule, 58 of them had at least one negative finding on Security Rule compliance**

McBRAYER

HIPAA Enforcement

- **On March, 21, 2016, OCR began the start of Phase 2 of audits, which will affect both Covered Entities and Business Associates**
  - **A revised audit protocol is now available, which provides CEs and BAs with more detailed elements and questions that should assist these entities with risk assessment**
    - **The protocol also breaks down what applies to CEs and BAs vs. what only applies to CEs**
    - 350 CEs and 50 BAs will be audited over a three-year period
      - BAs – 35 will be IT-related
      - 150 CEs and 50 BAs will be audited for Security Rule Compliance
      - 100 CEs will be audited for Privacy Rule Compliance
      - 100 CEs will be audited for Breach Notification Compliance

McBRAYER

Kentucky Privacy Laws

- Patient Access
  - Provide records when requested
    - 1st copy free
    - May charge up to $1/per page for additional copies
- Mental Health Records
  - To insurer, minimum necessary for payment or quality of care issues
  - 3rd parties may not re-disclose
  - Super confidential -written consent of all parties identified required for disclosure

McBRAYER

Kentucky Privacy Laws

- Sexually Transmitted Diseases
  - Providers required to report to health authorities
  - Super confidential -written consent of all parties identified required for disclosure
  - HIV/AIDS-
    - Super-duper confidential
- Substance Abuse
  - Super confidential -written consent of all parties identified required for disclosure
- Registries
  - Birth defects, cancer

McBRAYER

Professional Boards and Disciplinary Actions

- Maintaining patient confidentiality is a condition of licensure
  - KBML grounds for discipline
    - Willfully violated a confidential communication
      - KRS 311.595(16)
    - Unprofessional conduct
  - KBN grounds for discipline
    - Has violated the confidentiality of information or knowledge concerning any patient, except as authorized or required by law.
      - KRS 314.091(1)(n)
    - Unprofessional conduct

McBRAYER

Best Practices for HIPAA Compliance

- 1. Encrypt health information
- 2. Set up passwords or authentication requirements for software applications and devices
- 3. Do not allow gossip in your facility
- 4. Train all your staff members properly and thoroughly
- 5. Put incident response plans in place
- 6. Be vigilant about third-party business agreements
- 7. Avoid improper PHI disclosure
- 8. Designate a HIPAA champion

McBRAYER

Any questions?

Anne-Tyler Morgan
atmorgan@mmlk.com
(859) 231-8780, ext. 108

www.mmlk.com
www.mcbrayerhealthcare.com

McBRAYER