The New Alphabet Soup: HIPAA, PHI & BYOD

LeadingAge Maryland

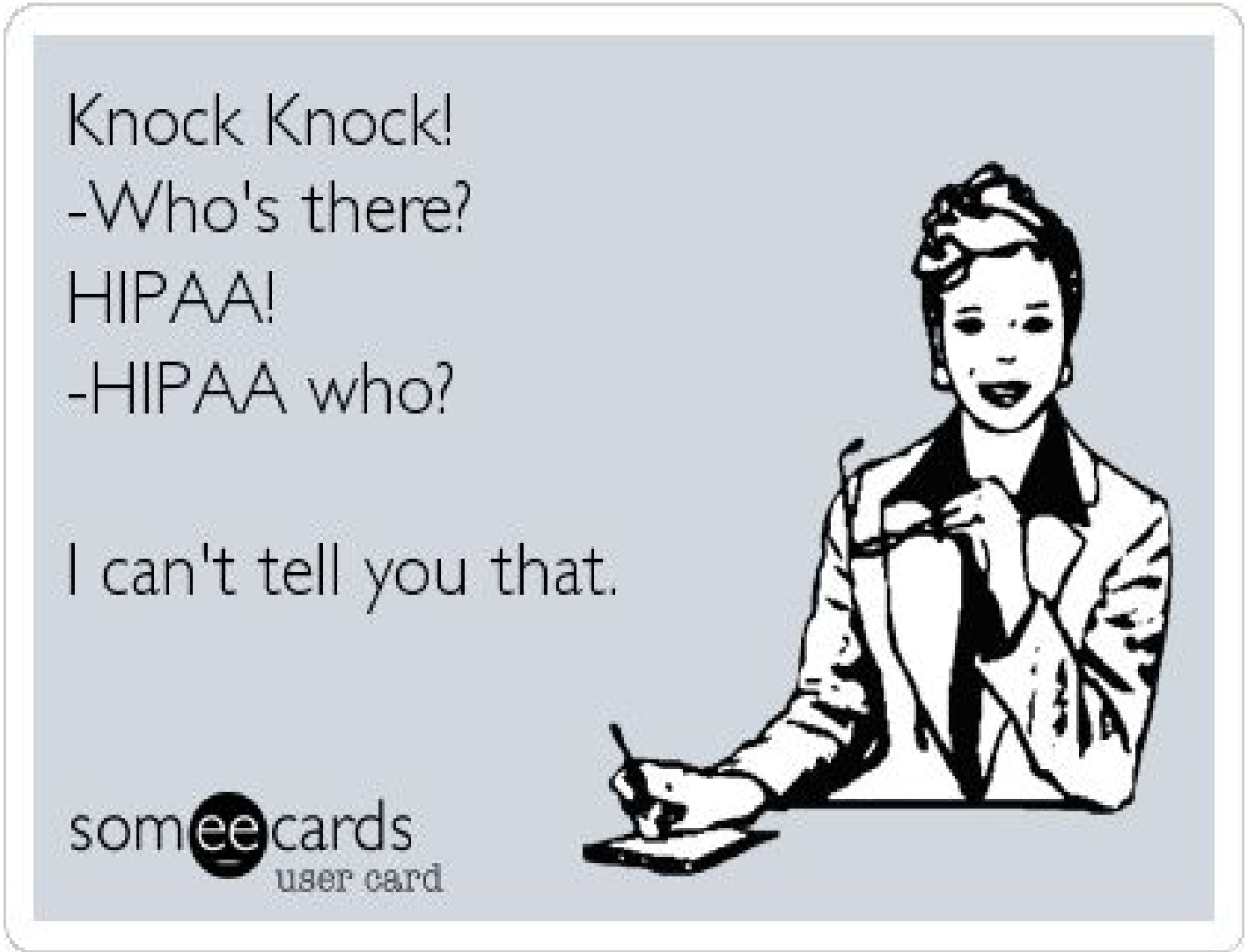
Clinical Education Day

May 19, 2016

Lauren Bicknese, CLCS

Objectives

- Understand and define HIPAA, PHI, & BYOD
- Identify proper and improper disclosures of PHI
- Identify the risks associated with employees' use of personal mobile devices in the workplace



Definitions

- HIPAA = Health Insurance Portability and Accountability Act of 1996
- PHI = Protected Health Information
  - ePHI = Electronic Protected Health Information
- BYOD = Bring Your Own Device

Understanding HIPAA

- Federal Law establishing standards and requirements for transmitting certain health information to improve the efficiency and effectiveness of the health care system while protecting patient privacy
- Privacy Rule: national standards to protect individuals' medical records and other personal health information
- Security Rule: national standards to protect individuals' electronic personal health information that is created, received, used or maintained

Who Does HIPAA Apply To?

- Covered Entities
  - Health Care Providers
    - Nursing Homes
    - Doctors, Clinics, Dentists, Pharmacies, etc.
  - Health Plans
    - Health Insurance Companies, HMOs, Employee Sponsored Health Plans
  - Health Care Clearinghouses
- Business Associates
  - Perform a function on behalf of a covered entity involving the use of PHI

Is your Facility a CE or Not?

- Do you transmit health information electronically using standard transactions?
- Do you bill or check health plan benefit eligibility electronically?
- Do you submit electronic claims for medical care to a healthcare insurer, such as Medicare, Medicaid, or a private insurer, for payment? Or use a third party for billing?
- Is your facility part of a hospital and nursing home considered one legal entity?
- Does your facility include a clinic with physicians who provide healthcare treatment to residents?

What Does HIPAA Apply To?

- PHI
  - Individually identifiable health information
- ePHI
  - PHI transmitted electronically or maintained in electronic media

What is PHI?

- “Individually identifiable health information” held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral
- Information, including demographic data, that identifies the individual and that relates to:
  - An individual’s past, present or future physical or mental health or condition
  - The provision of health care to an individual
  - The past, present, or future payment for the provision of health care to an individual
- Created or received or maintained by a covered entity or business associate

PHI “Identifiers”

- Names
- Geographic information
- Dates
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers & serial numbers, including license plate numbers
- Device identifiers & serial numbers
- URLs
- IP address numbers
- Biometric identifiers
- Full-face photographic images and any comparable images
- Other unique identifying numbers, characteristics, or codes

Types of Data Collected

Table 1: Twenty-six data elements that healthcare organizations may collect and store about patients in electronic files or records.

Data types	Pct%	Data types	Pct%
Name	99%	Health insurance information	58%
Gender	98%	Social Security Number	52%
Address	96%	Prescription drugs	38%
Telephone	96%	Educational background	34%
Personal health history	95%	Race	31%
Family health history	92%	Addictions	31%
Age	92%	Interest in clinical trial research	29%
Physical characteristics	90%	Sexual preferences	26%
Employer	80%	Photo	23%
Guardian or next of kin	76%	Diet	20%
Marital status	75%	Credit history	16%
Credit card or bank payment information	74%	Religion	15%
Names of primary health care provider	62%	Ethnicity	13%

Source: Ponemon Institute, Electronic Health Information at Risk: A Study of IT Practitioners, 10-15-2009

Permitted Uses & Disclosures of PHI

1. To the Individual
2. Treatment, Payment, Health Care Operations (TPO)
3. Uses and Disclosures with Opportunity to Agree or Object
4. Incidental Use and Disclosure
5. Public Interest and Benefit Activities
6. Limited Data Set

Use = the sharing, employment, application, utilization, examination, or analysis of PHI *within* the covered health care component that maintains the PHI

Disclosure = the release, transfer, provision of, access to, or divulging in any manner PHI *outside of* the covered health care component that maintains the PHI

Non-Permitted Uses & Disclosures of PHI

- NON-TPO purposes, i.e. a vendor's request for residents on a specific drug
- Psychotherapy notes
- Research requests without an IRB approval
- Marketing
- Fundraising

These situations require a patient's written authorization prior to the use or disclosure of PHI.

Limiting Use & Disclosures to the Minimum Necessary

- Staff access to PHI must be role-based, i.e. based on job duties, “need to know” basis
- Staff must exercise reasonable efforts not to use or disclose more than the minimum amount of information needed to accomplish an intended purpose

HIPAA Rules Apply to PHI When…

- You use it
- You disclose it
- You store it
- You see it on your computer
- It is lying on your desk
- You share it with another health care provider
- You share it with another contracted service provider
- You are talking about it face-to-face, in any public area
- You are talking about it over the phone

Disclosure to Authorized Personal Representatives

- Use professional judgment and experience
- A resident's objections to disclosures must be honored
- Minimum necessary standard applies…
  - Notification: to locate or identify a family member, relative, or close personal friend involved in the resident's care
  - Involvement: PHI relevant to the person's involvement in the resident's care, i.e. pick-up prescriptions, medical supplies, x-rays
  - Payment: payment for healthcare services
- Note: Decedent's Rights
  - PHI may only be disclosed without authorization to:
    - Coroner or medical examiner; funeral director; law enforcement

Examples

- Clinician request for PHI
  - No limitations for physicians/care providers *directly* or *indirectly* involved in the care of the resident
  - Physicians/care providers may disclose PHI to consulting/referring physicians
  - No disclosure permitted to clinicians who do not have TPO responsibilities for the resident!

Permitted or Non-Permitted PHI Requests?

- A clinician requests access to family member's PHI (not a designated personal representative)
- A pharmacy rep requests a list of residents on a treatment regimen for marketing purposes
- Non-clinician staff member requests access to family member's PHI (not a designated personal representative)

Permitted or Non-Permitted PHI Requests?

- Medical students who participated in a resident's care write up the case for presentation at rounds
- A doctor discusses a resident's treatment in front of a resident's friend that the resident asked to come into the treatment room
- A doctor gives information about a resident's mobility limitations to the resident's daughter who is driving the resident off-site
- A healthcare provider shares information with an interpreter who works for the provider
- A nursing facility discusses a resident's bill with the resident's adult daughter who is present with the resident and has questions about the charges
- A nursing facility discusses a resident's bill with her adult son who calls with questions about charges to his mother's account

HIPAA Security Standards

- Security Management Process
  - Security Official
  - Risk Analysis
  - Risk Management
  - Sanction Policy
  - Information System Activity Review

HIPAA Security Standards

- Safeguards
  - Workforce
  - Information Access
  - Facility Security Plan
  - Workstation Use
  - Device & Media Controls
  - Access Controls (Technical)

HIPAA Security Standards

- Workforce & Information Access
  - Authorization & Supervision
  - Workforce Clearance
  - Termination Procedures
  - Access Authorization
  - Access Establishment & Modification

- Workforce Training
  - New employees or contractors
  - Due to changes

HIPAA Security Standards

- Facility Security & Workstation Use
  - Security Plan
  - Control and Validation
  - Maintenance Records
  - Acceptable Uses of Computer Technology
    - Passwords not shared
    - Business Purposes Only

HIPAA Security Standards

- Device & Media Controls
  - Disposal
  - Re-use
  - Accountability
  - Backup & Storage

HIPAA Security Standards

- Audit Controls & Integrity
  - Audit records maintained for review
    - Hardware & Software
    - Active Users
    - Login Monitoring
    - Additions, deletions, and sanitization of media
    - Transportation to and from storage facilities
  - Integrity Controls
    - Virus Protection
    - Revision Control

HIPAA Security Standards

- Events Requiring Action
  - Security Incidents & Reporting
  - Sanctions
  - Breach Notification

What is a Breach?

- Events Requiring Action
  - “the acquisition, access, use, or disclosure of PHI in a manner”
    - Not permitted under HIPAA
    - Compromising the security or privacy of PHI
  - Must constitute a violation of the Privacy Rule
  - Assumed, unless it can be proved there is a “low probability” of harm to an individual

Penalties

Offense	General Penalty
Civil Violation	$100/offense; up to $1.5M/year
Wrongful Action	$50,000/offense; 1 year in prison
False Pretense	$100,000/offense; 5 years in prison
Intent to Sell	$250,000/offense; 10 years in prison

Key Takeaways - Security of PHI

- Password security
  - Systems and devices
  - Strong passwords; change routinely per policy
  - Do not share passwords
- Lock computer and devices – don't leave PHI visible!
- Properly dispose of paper records and PHI stored on electronic devices
- Use caution when faxing
  - Verify number
  - Use cover sheets
- Utilize key access to file rooms/cabinets
- Enable automatic log-offs

BYOD: Definitions

- **eHealth**: the use of electronic information and communication technologies for health-related services.
- **mHealth**: mobile health; the practice of medicine and public health supported by mobile devices.
- **BYOD**: a policy in which employees are allowed to use their personal mobile devices to access enterprise data systems.

Benefits of BYOD

- Employee Satisfaction – motivated workforce!
- One Device vs. Two
- Cutting-Edge Devices
- Less Expense for an Employer
- Higher Productivity Levels
- Improved Customer Service

Risks of BYOD

- Data Security
- e-Discovery
- Personal Injury
- Data Corruption and Deletion
- Device Sharing
- Revoked or Lost Devices
- Compensation Issues

Issues to Consider

- Changing How Caregivers Communicate
- Digital Distractions Affect Care
- Display Limitations
- Security Breaches
- Smartphone Cameras
- Power-Cord-Related Issues
- Increased Traffic on the Wi-Fi Network
- Cross-Contamination
- Support Considerations

Issues to Consider

- Is mobile access a must?
- What are the goals and benefits of implementing a BYOD program?
- Which group of your workforce needs mobile access and to what data or systems?
- Has a full risk assessment been performed, including assessing the legal issues surrounding BYOD?
- Will BYOD require the company to establish new HR policies?
- Will BYOD affect infection control?
- How will you address employee privacy concerns?

Risk Management Solutions

- Mobile Security Expert
- BYOD Policies and Procedures
- Access Control
- Malware and Antivirus
- Geofencing
- MDM, or Mobile Device Management

What's Happening IRL (In Real Life)

- "Nursing Home Workers Share Explicit Photos of Residents on Snapchat"
- "Two charged with elder assault at an assisted-living facility"
- "Nursing Home Workers Fired for Snapchat Video Mocking Elderly Resident"
- Springhill Senior Residence – SNF in Mobile, Alabama
  - CMS interpretation of SOM standards – sections 483.10(e) and 483.75(1)(4)
    - "staff must examine and treat residents in a manner that maintains the privacy of their bodies"
    - "keep confidential" defined as "safeguarding the content of information including video, audio, or other computer stored information from unauthorized disclosure without the consent of the individual and/or the individual's surrogate or representative"

In Summary

- Limit PHI use and disclosures to those specifically allowed by HIPAA or get the individual's written authorization.
- If you are not sure if a use or disclosure is allowed, refer to Privacy Official.
- Develop a BYOD policy and make sure staff is aware of it.
- Auto-lock devices, enable remote wiping, and be aware of your surroundings when using mobile devices to access ePHI.
- Report possible PHI breaches to Privacy Official.
- Report incidents of lost/stolen devices to IT.

Thank you for your time and attention!

Lauren Bicknese

lbicknese@rcmd.com