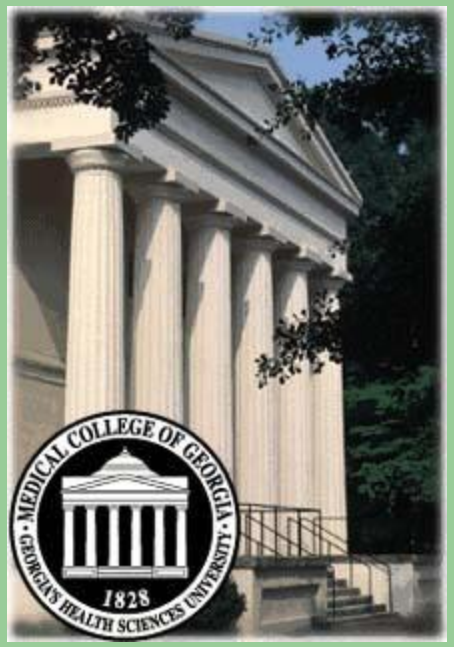
Privacy and Information Security Awareness Training



Health Insurance Portability & Accountability Act of 1996 -- HIPAA

Objectives

- Understand basic HIPAA requirements
- Understand how the MCG Health System implements HIPAA regulations
- Best Practice and Scenarios

The Hippocratic Oath declares:

"Whatever, in connection with my profession, or not in connection with it, I may see or hear in the lives of men which ought not be spoken abroad I will not divulge as reckoning that all should be kept."

HIPAA is a bit more specific….

Health Insurance Portability & Accountability Act of 1996 (HIPAA)

- **Primary Goal: Improve portability and continuity of health insurance coverage, combat fraud and abuse, and help control administrative costs of health care**
- **Standardized Electronic Data – October 2002**
- **Privacy – April 2003**
- **Security – April 2005**

Need for Privacy and Security Standards

- To receive accurate and reliable diagnosis and treatment, patients must provide accurate, detailed information about their personal health, behavior, and other aspects of their lives.
- Health care providers rely on this information to process claims, coordinate care (portability) and for other administrative functions
- Individuals are concerned how their information is used.
- Patients want to know that their sensitive information will be protected.

Privacy Law -- April 2003

- The Privacy Rule sets standards for **uses** and **disclosures** that are **authorized** or **required** and what **rights** patients have with respect to their protected health information (PHI)
- The Privacy Rule applies to PHI **in any form:**

  Paper - Electronic - Oral

Security Law -- April 2005

- The Security Rule sets standards for basic **safeguards** to prevent unauthorized access, alteration, deletion, and transmission
- These basic safeguards are to protect the **confidentiality, integrity,** and **availability** of electronic PHI
- The Security Rule applies only to PHI in **electronic form**

Beyond HIPAA Requirements

- **Where state law is more strict than HIPAA, covered entities must adhere to state law**
- **Law pertaining to Mental Health, Substance Abuse and AIDS / HIV provide additional limitations beyond HIPAA**

HIPAA Vocabulary

- **Authorized** means that, except as otherwise permitted (TPO) or required, the entity may not use or disclose PHI without a valid request to release PHI. (Format available through HIMS Dept.)
- **Disclosure** means the release, transfer, provision of access to, or divulging of information **outside** the covered entity
- **Required Disclosures** means a release of PHI **authorized by law;** patient authorization is not necessary.
- **Security incident** means an attempted or successful **unauthorized access, use, disclosure, modification, or destruction of information or interference** with system operations in an information system

HIPAA Vocabulary

- **TPO means treatment, payment, or health care operations (Consulting/referring clinicians, used in providing patient's care, billing, teaching, accreditation, compliance, research, etc).**

  Note: Clinical research is considered an operational use but requires approval by an IRB

- **Use means the sharing, employment, application, utilization, examination, or analysis of individually identifiable information within the health care provider's organization**

Defining PHI

- **Protected Health Information (PHI)** is "individually identifiable health information created or maintained by a covered entity, relates to past, present, or future physical or mental condition for provision of health care, and includes demographic information."
- **Protected Health Information (PHI)** is individually identifiable health information that is created or received by the MCG Health System.

Examples of PHI (Puzzle pieces)

- Name
- SSN
- Driver's License
- Address
- Marital Status
- Financial Information
- Income
- Parental Status
- Gender
- Race
- Religion
- Medical Condition
- Test Results

De-Identified Data

When all identifiers are removed, the information is no longer considered PHI, and therefore, no longer governed under HIPAA.

Patient Privacy Rights

- **Right to know the terms of the covered entity's Notice of Privacy Practice (NPP)**
- **Right to know what has been disclosed and to whom (permitted or required disclosures); requires written request**
- **Right to request an amendment to PHI; requires written request**

More Patient Privacy Rights

- Right to request **restrictions** (opt out of directory); requires written request
- Right to request **confidential communications**; requires written request
- Right to **inspect** and **request copies** of PHI; requires written request

Exception: In some circumstances a request for access or copies of psychotherapy notes may be denied.

Minimum Necessary

§ 164.502 (b) Standard: minimum necessary

When **using** or **disclosing** PHI or when **requesting** PHI from another covered entity, a covered entity must make **reasonable efforts to limit PHI** to the minimum necessary to accomplish the **intended purpose** of the use, disclosure, or request.

Use and Disclosure is limited to Minimum Necessary

- PHI should be **seen** by only those who are authorized to see it
- PHI should be **heard** by only those who are authorized to hear it
- PHI should be **transmitted or shared** with those who are authorized to receive it

Exception to Minimum Necessary

When release of PHI is for diagnosis or treatment purposes, anything might be relevant and minimum necessary does not apply

Reasonable Due Diligence

- Important to verify a requestor's identity and authority, but this process should not impede patient care

- Professional judgment and reasonableness are required by HIPAA – and should be liberally applied

Incidental Disclosures

Even when reasonable steps to safeguard the privacy of PHI are taken, it must be recognized that certain disclosures may occur.

- **Calling out a name in the waiting room**
- **During the course of a treatment session, or during a visit to a hospital room, sometimes it is possible to overhear a discussion involving PHI**

.

HIPAA Compliance

- No “HIPAA Police”
- Enforcement is complaint-driven thru Office of Civil Rights
- Privacy and Security Officers
- Covered entity must identify and resolve issues
- Sanctions

Office of Civil Rights

“can't fine a covered entity when the failure to comply is "due to reasonable cause and not willful neglect,"

-O.C.R. Director Rick Campanelli

Penalties for Non- Compliance Civil and Criminal sanctions

- **$100 fine per day for each unmet standard. (Up to $25,000 per person, per year, per standard)**
- **$50,000 fine + one year in prison for knowingly disclosing health information for improper use or to unauthorized entities**
- **$100,000 fine + five years in prison for obtaining health information under false pretenses**
- **$250,000 fine + ten years in prison for using health information to sell, transfer, or use for commercial advantage, personal gain, or malicious harm**

Five Most Common Types of Complaints Involve Direct Contact – OCR

May, 2005

(1) Impermissible disclosures (e.g., gossiping to a friend outside the hospital about the medical condition of a neighbor who is a patient);

(2) Lack of adequate safeguards (e.g., leaving files around, not protecting PHI on computer screens);

(3) Refusal or failure to provide access to — or a copy of — medical records;

(4) Disclosure of more than the minimum necessary protected health information; and

(5) Failure to include valid language in patient authorizations for PHI disclosures.

HIPAA and the MCG Health System

What is an OHCA?

- **Organized Health Care Arrangement**
- **MCG Health System - Clinically integrated**
- **MCG**
- **MCGHI**
- **PPG**

Notice of Privacy Practices (NPP)

- **NPP is used jointly by MCG, MCGHI, and PPG**
- **NPP clinically integrates PHI**
- **NPP allows for sharing of PHI within the OHCA for treatment, payment, & operations (TPO)**

NPP: Blueprint for Rights, Uses, Disclosures

- **Patient Rights**
- **Each Entity responsible for its own activities**
- **Use: Sharing within OHCA for treatment including involving family, prevent serious threat to health or safety, sending PHI to referring physician for continuity of care, sending a bill to insurance company, teaching students, evaluating job performance, compliance, HAC approved clinical research**

NNP Continued

- **Use or Disclosure without permission:**

  Public Health Purposes, Recalls, Abuse, Neglect, Domestic Violence, Audits or Inspections, Approved Research Studies, Funeral arrangements, Organ Donations, Government programs, Workers' Comp, Emergencies, National Security

  Consider documenting in record

  Call MCG Privacy Officer concerning National Security issues

NNP Continued

- Required Disclosures:

  Law enforcement: Crimes committed on MCG Health System campus, Crimes against patients, faculty, staff or students

  Judicial Inquiries: Subpoenas, Court Orders

  Call MCG Privacy Officer

  Accounting of Disclosures

NNP Continued

- Address questions to Privacy Officer or Program Management Office
- Request Forms from PMO
- File complaints with MCG Health System through PMO or contact the Office of Civil Rights
- Compliance Hotline Information

Non- OHCA Entities

- No joint NPP - Not clinically integrated
- No sharing of PHI

- MCG School of Dentistry
- MCG Student Health Services
- Georgia War Veterans Nursing Home
- Georgia Correctional Health Care*****

  * Exception to the rule – No NPP required

What do Privacy and Security Officers do?

- Oversee the implementation of privacy and security compliance
- Advise faculty, employees and students on privacy and security issues
- Receive and respond to complaints or inquiries
- Coordinate compliance with OHCA and Non-OHCA entities
- Train faculty, employees, and students
- Maintain record of reported violations, and responsive actions taken

Watch Dogs on Campus: Labrador Retrievers

Your questions, comments and feedback are welcomed

Please consider the HIPAA Privacy Officer and the Security Officer as resources

Christine Adams
Privacy Officer
HS 3135
706-721- 5631

chradams@mcg.edu

Mark Staples
Security Officer
HS 2125
706-721-1577

mstaples@mcg.edu

Who You Gonna Call?

- **MCG Health Care System Compliance Hotline 1-800-576-6623**

- **A description of the concern**
- **Who is involved**
- **Where and when the incident took place**
- **Your name and contact number – Optional**
- **Whistle-Blower Protection**

Best Practices

- Role-based access or User-based access to ensure minimum necessary
- Clean desk policy
- Placing medical charts with name faced inward in chart holder
- Turning monitors away from general public
- Restricting access to areas where PHI is openly displayed

More Best Practices

- Conduct conversations in areas apart from others
- When referencing a document, don't show document to another if there is information that the other should not have
- Take the organization's name and main number, the caller's name and the caller's extension number. Hang up then call them back

Even More, Best Practices

- To confirm a caller is who they say they are, check the individual's record and confirm details such as DOB, address, health plan number
- Lock offices or desks
- Shredding documents rather than putting them in the trash
- Verify the email address before sending

Still More, Best Practices

- Confirm with the receiver that the receiver's email account is password protected
- Use encryption when sending PHI
- Never send PHI off-campus using electronic mail
- Put a password challenge on all spreadsheets, word processing documents, and databases

Last Best Practice Examples

- Store all data on a network file server that is backed up regularly
- Safeguard information stored so that only those that need to have access are able to access (In a folder on a network file server that is restricted to appropriate personnel)
- Add a password challenge to all screensavers on computers that access PHI and set the idle time to less than 5 minutes
- Keep computer operating systems up-to-date and running active antivirus software

Scenarios

- **Health care provider accesses his own electronic health record**
- **Physician is admitted to an acute care hospital, fellow concerned clinicians attempt to follow patient's course by accessing the system**
- **Celebrity enters hospital, curious staff access sensitive information**

Resources

- MCG Privacy and Security Officers
- MCG Office of Institutional Audit & Compliance
- MCGHI Compliance / HIPAA PMO
- MCG / MCGHI Policies and Procedures
- Federal and State Laws Regulations

Questions???