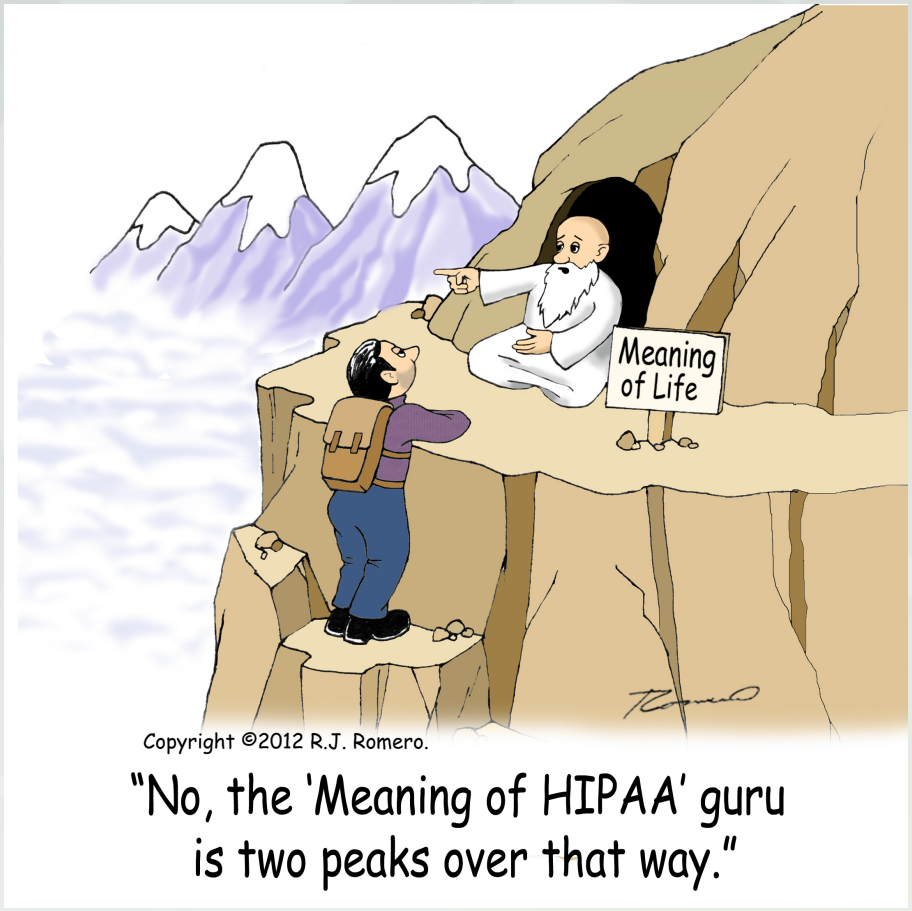
Overview of the HIPAA Privacy Rule



MICHIGAN STATE UNIVERSITY HEALTHTEAM

Objectives

- Learn about the importance of the HIPAA Privacy and Security Rules in safeguarding patient confidentiality.
- Recognize situations in which protected health information may be disclosed improperly.
- Appreciate the consequences of HIPAA rule and MSU policy violations.

Basic Principle: Privacy Rule

A major purpose of the HIPAA Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. The **essence of the rule** is:

A covered entity may not use or disclose protected health information, except either:

(1) as the Privacy Rule permits or requires; or

(2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

45 CFR 164.502

"Covered Entities"

Health care provider groups such as MSU HealthTeam are subject to HIPAA and thus referred to as "covered entities." Since HealthTeam and other covered entities on campus are not legally separate from the rest of the university, MSU is considered a "hybrid entity."

"I wanted to be a zombie, but dad works for some government agency and he said it would be scarier to dress as something called a 'Covered Entity under HIPAA'."

“Protected Health Information”

The Privacy Rule protects all "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.

The Privacy Rule calls this information “*protected health information (PHI).”*

"Protected Health Information"

PHI includes any information related to:

1. The individual's past, present or future physical or mental health and condition.
2. The provision of health care to the individual.
3. The past, present or future payment for the provision of health care to the individual.

PHI includes many common identifiers such as names, addresses, telephone numbers, images, MRNs and other unique identifying numbers, characteristics, or codes.

"Use" / "Disclosure"

"**Use**" means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information **within an entity** that creates or maintains such information.

"**Disclosure** " means the release, transfer, provision of, access to, or divulging in any other manner of information **outside the entity** holding the information.

Permitted Uses & Disclosures

A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:

1) To the Individual
2) Treatment, Payment, and Health Care Operations
3) **Opportunity to Agree or Object;**
4) **Incident to an otherwise permitted use and disclosure;**
5) Public Interest and Benefit Activities; and
6) Limited Data Set for the purposes of research, public health or health care operations.

Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

Patient Rights

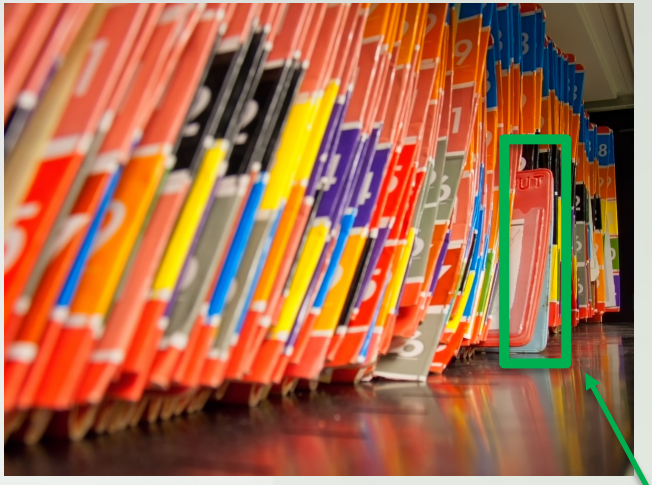
1. Covered entities must distribute a "**Notice of Privacy Practices**."
2. **Access**: Patients have the right to review and receive copies of their information in the covered entities "designated record set" with some exceptions, such as psychotherapy notes, information compiled for legal proceedings and certain laboratory results designated by other laws. Professionals may deny access to prevent harm to the individual or others.
3. **Amendment** Individuals may request to amend (not alter) their records if they are inaccurate or incomplete.
4. **Disclosure Accounting** Individuals have the right to "an accounting of disclosures" of their records for the six years prior to their requests, with a whole host of exceptions (including treatment/payment/operations.)
5. **Restriction requests** for treatment/payment/operations may be made by individuals but the covered entity is under no obligation to comply, **except in the case of disclosures to health plans when patients have paid 100% "out of pocket for the service."**

Minimum Necessary Standard

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

Example Exceptions:

1. Treatment
2. Patient Access to Own Records
3. Written Authorizations
4. Legal & HHS Requirements



*The minimum amount of PHI needed to get the (authorized) job done, or just this chart.

Breaches


Copyright © 2012 R.J. Romero.
"We accidentally emailed your test results to the County Coroner. He's not sure what's wrong with you, but he'll know more after the autopsy."

Breaches

An unauthorized acquisition, access, use or disclosure of PHI is presumed to be a breach *unless* the covered entity or its business associate *demonstrates* that there is a low probability that the protected health information has been compromised.

Breaches

Breach Notification Process

- Covered entities write letters to the affected individual(s) that must include a brief description of what happened, types of information involved, steps to limit the harm, mitigation efforts and contact information.
- Breaches are reported to HHS. If under 500 patient records are involved, the covered entity maintains a log and submits it annually. If a breach affects 500 or more individuals, the covered entity must notify HHS and local media without unreasonable delay.

"Wall of Shame"

Breaches involving 500 or more patients are listed on the OCR web site.

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	City of Detroit	MI	Healthcare Provider	544	02/05/2018	Loss	Other Portable Electronic Device
	MidMichigan Medical Center-Alpena	MI	Healthcare Provider	1900	12/19/2017	Loss	Paper/Films
	Bronson Healthcare Group	MI	Healthcare Provider	8256	12/05/2017	Hacking/IT Incident	Email
	Eclectic Chiropractic Rehab	MI	Healthcare Provider	650	12/05/2017	Unauthorized Access/Disclosure	Email
	Henry Ford Health System	MI	Healthcare Provider	43563	12/01/2017	Theft	Email
	McLaren Medical Group, Mid-Michigan Physicians Imaging Center	MI	Healthcare Provider	106008	08/24/2017	Hacking/IT Incident	Network Server
	Spectrum Health System	MI	Healthcare Provider	902	08/03/2017	Theft	Other Portable Electronic Device
	Detroit Medical Center	MI	Healthcare Provider	1529	07/13/2017	Theft	Desktop Computer, Paper/Films
	Henry Ford Health System	MI	Healthcare Provider	596	06/26/2017	Theft	Paper/Films
	Airway Oxygen, Inc.	MI	Healthcare Provider	500000	06/16/2017	Hacking/IT Incident	Network Server
	Michagan Facial Aesthetic Surgeons d/b/a University Physician Group	MI	Healthcare Provider	3467	04/28/2017	Theft	Laptop
	Memorial Healthcare	MI	Healthcare Provider	685	04/03/2017	Unauthorized Access/Disclosure	Other
	Singh and Arora Oncology Hematology, P.C.	MI	Healthcare Provider	16000	10/21/2016	Hacking/IT Incident	Network Server
	North Ottawa Medical Group	MI	Healthcare Provider	22000	06/09/2016	Unauthorized Access/Disclosure	Network Server
	Family & Children's Services of Mid Michigan, Inc.	MI	Healthcare Provider	981	04/27/2016	Hacking/IT Incident	Network Server
	W. Christopher Bryant DDS PC	MI	Healthcare Provider	2200	03/17/2016	Loss	Other Portable Electronic Device

Social Media

It is never OK to post a patients picture or discuss any details online without their express authorization. Clinics with their own Facebook pages and Twitter accounts should check with the Marketing & Communications Manager to make sure the proper permissions are in place.

HIPAA Enforcement

If a covered entity or a business associate is determined to be in violation of the HIPAA rules, the HHS Office of Civil Rights (OCR) may provide technical assistance, access civil monetary penalties, and take even more strict actions depending on the circumstances.

- Civil monetary penalties (CMP) range from $100 to $50,000 *per violation* on the level of culpability; up to an annual maximum of $1.5 million for identical violations.
- Typically the OCR and the covered entity/business associate will enter into a resolution agreement that involves a settlement less than the maximum CMP, with a multi-year corrective action plan that also has costs.
- From the beginning of enforcement in 2003 until the end of 2017, OCR has settled or imposed a CMP in 53 cases for a total dollar amount of $75,229,182.00
- The OCR also referred 664 cases during this time to the Department of Justice for criminal prosecution.

Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History

October 15, 2018

Anthem, Inc. has agreed to pay $16 million to the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) and take substantial corrective action to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules after a series of cyberattacks led to the largest U.S. health data breach in history and exposed the electronic protected health information of almost 79 million people.

The $16 million settlement eclipses the previous high of $5.55 million paid to OCR in 2016.

Department of Justice

U.S. Attorney's Office

Middle District of Florida

FOR IMMEDIATE RELEASE

Wednesday, August 3, 2016

Former Tampa-Area Hospital Employee Sentenced For Stealing Patient Information And Filing Fraudulent Tax Returns

Tampa, Florida – U.S. District Judge Susan C. Bucklew today sentenced Shanakia Benton to three years in federal prison for wrongful disclosure of individual identifiable health information and wire fraud. As part of her sentence, the Court also entered a money judgment in the amount of $77,239, the proceeds of the wire fraud. Benton pleaded guilty on May 2, 2016.

According to court documents, Benton was an employee at Tampa General Hospital (TGH) and had access to the personal health information of thousands of patients. She regularly received training regarding the Health Insurance Portability and Accountability Act, which prevents the unauthorized disclosure of personal health information. Despite her training, between June 2011 and December 2012, Benton illegally accessed the personal information of more than 600 TGH patients. Benton and her accomplices then used that information to file at least 29 false tax returns seeking refunds totaling $226,000.

This case was investigated by the U.S. Department of Health and Human Services – Office of Inspector General, the Federal Bureau of Investigation, the Internal Revenue Service – Criminal Investigation, and the Tampa Police Department. It was prosecuted by Trial Attorney Timothy Loper.

Topic:
Financial Fraud
Identity Theft
StopFraud

USAO - Florida, Middle

Updated August 3, 2016

FOR IMMEDIATE RELEASE
November 26, 2018

Contact: HHS Press Office
202-690-6343
media@hhs.gov

Allergy practice pays $125,000 to settle doctor's disclosure of patient information to a reporter

Allergy Associates of Hartford, P.C. (Allergy Associates), has agreed to pay $125,000 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and to adopt a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Allergy Associates is a health care practice that specializes in treating individuals with allergies, and is comprised of three doctors at four locations across Connecticut.

In February 2015, a patient of Allergy Associates contacted a local television station to speak about a dispute that had occurred between the patient and an Allergy Associates' doctor. The reporter subsequently contacted the doctor for comment and the doctor impermissibly disclosed the patient's protected health information to the reporter.

OCR's investigation found that the doctor's discussion with the reporter demonstrated a reckless disregard for the patient's privacy rights and that the disclosure occurred after the doctor was instructed by Allergy Associates' Privacy Officer to either not respond to the media or respond with "no comment." Additionally, OCR's investigation revealed that Allergy Associates failed to take any disciplinary action against the doctor or take any corrective action following the impermissible disclosure to the media.

HHS.gov

U.S. Department of Health & Human Services

Health Information Privacy

HIPAA for Individuals | Filing a Complaint | HIPAA for Professionals | Newsroom

- Privacy +
- Security +
- Breach Notification +
- Compliance & Enforcement −
  - Enforcement Rule
  - Enforcement Process
  - Enforcement Data
  - Resolution Agreements
  - Case Examples
  - Audit
  - Reports to Congress
  - State Attorneys General
- Special Topics +
- Patient Safety +
- Covered Entities & Business Associates +
- Training & Resources
- FAQs for Professionals

Multiple alleged HIPAA violations result in $2.75 million settlement with the University of Mississippi Medical Center (UMMC)

The University of Mississippi Medical Center (UMMC) has agreed to settle multiple alleged violations of the Health Insurance Portability and Accountability Act (HIPAA) with the U.S. Department of Health and Human Services, Office for Civil Rights (OCR). OCR's investigation of UMMC was triggered by a breach of unsecured electronic protected health information ("ePHI") affecting approximately 10,000 individuals. During the investigation, OCR determined that UMMC was aware of risks and vulnerabilities to its systems as far back as April 2005, yet no significant risk management activity occurred until after the breach, due largely to organizational deficiencies and insufficient institutional oversight. UMMC will pay a resolution amount of $2,750,000 and adopt a corrective action plan to help assure future compliance with HIPAA Privacy, Security, and Breach Notification Rules.

"In addition to identifying risks and vulnerabilities to their ePHI, entities must also implement reasonable and appropriate safeguards to address them within an appropriate time frame," said OCR Director Jocelyn Samuels. "We at OCR remain particularly concerned with unaddressed risks that may lead to impermissible access to ePHI."

On March 21, 2013, OCR was notified of a breach after UMMC's privacy officer discovered that a password-protected laptop was missing from UMMC's Medical Intensive Care Unit (MICU). UMMC's investigation concluded that it had likely been stolen by a visitor to the MICU who had inquired about borrowing one of the laptops. OCR's investigation revealed that ePHI stored on a UMMC network drive was vulnerable to unauthorized access via UMMC's wireless network because users could access an active directory containing 67,000 files after entering a generic username and password. The directory included 328 files containing the ePHI of an estimated 10,000 patients dating back to 2008.

Further, OCR's investigation revealed that UMMC failed to:

- implement its policies and procedures to prevent, detect, contain, and correct security violations;
- implement physical safeguards for all workstations that access ePHI to restrict access to authorized users;
- assign a unique user name and/or number for identifying and tracking user identity in information systems containing ePHI; and
- notify each individual whose unsecured ePHI was reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach.

The University of Mississippi paid a $2.75 million settlement to OCR and agreed to corrective action for a breach that affected 10,000 people. The lack of timely and reasonable safeguards to enforce the HIPAA privacy and security rules also influenced the enforcement action.

New York Presbyterian and Columbia University paid $4.8 million to HHS to settle a HIPAA violation Case.

The ePHI of 6,800 individuals (including patient status, vital signs, medications, and laboratory results) was breached after a physician deactivated a server and accidently made the data available on the Internet.

FOR IMMEDIATE RELEASE
May 7, 2014

Contact: HHS Press Office
202-690-6343
media@hhs.gov

Data breach results in $4.8 million HIPAA settlements

Two health care organizations have agreed to settle charges that they potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to secure thousands of patients' electronic protected health information (ePHI) held on their network. The monetary payments of $4,800,000 include the largest HIPAA settlement to date.

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) initiated its investigation of New York and Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report, dated September 27, 2010, regarding the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results.

NYP and CU are separate covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP. The entities generally refer to their affiliation as "New York Presbyterian Hospital/Columbia University Medical Center." NYP and CU operate a shared data network and a shared network firewall that is administered by employees of both entities. The shared network links to NYP patient information systems containing ePHI.

The investigation revealed that the breach was caused when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient ePHI. Because of a lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on internet search engines. The entities learned of the breach after receiving a complaint by an individual who found the ePHI of the individual's deceased partner, a former patient of NYP, on the internet.

HIPAA Questions?

Contact

John Hazewinkel, MPA, JD
Compliance & HIPAA Privacy/Security Officer
West Fee 415
(517) 355-1822
John.Hazewinkel@hc.msu.edu

See: http://www.hhs.gov/hipaa/index.html