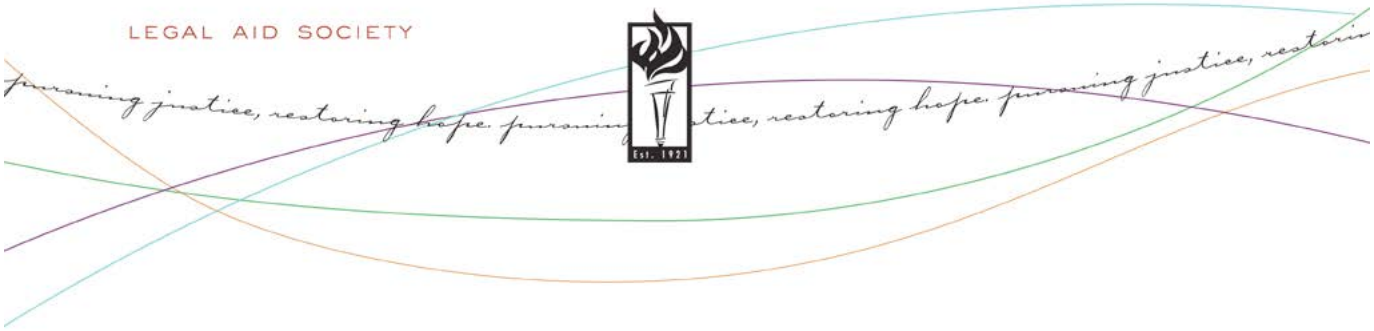
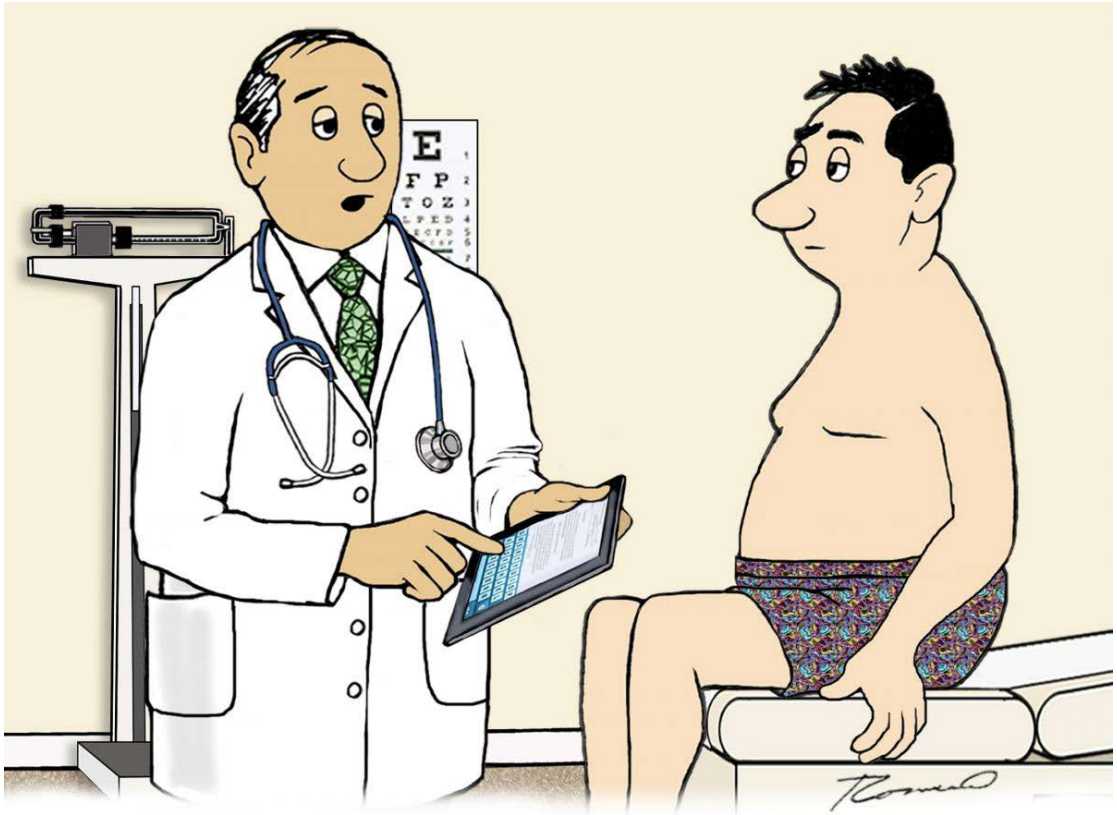
WRAPPING YOUR HEAD AROUND HIPAA PRIVACY REQUIREMENTS

Jeffrey Staton
Attorney at Law
Legal Aid Society of Louisville
416 W. Muhammad Ali Blvd., Ste. 300
Louisville, KY 40202
Phone: 502.614.3146
Jstaton@laslou.org



HIPAA: JUST A FEW BASICS



"According to your HIPAA release form
I can't share anything with you."

What is HIPAA?

- HIPAA is a 1996 Federal Law.
- Acronym for Health Insurance Portability & Accountability Act of 1996 (45 C.F.R. parts 160 & 164).
- Provides a framework for establishment of nationwide protection of patient confidentiality, security of electronic systems, and standards and requirements for electronic transmission of health information.

The HIPAA Privacy Rule

- The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. **The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.** The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

Who Does HIPAA Apply to?

- Covered Entities: A covered entity is any person, business or institution that provides healthcare or keeps medical records on patients.
- Business Associates: Around January 2013, HIPAA was expanded to cover business associates of covered entities. These are contractors and subcontractors of covered entities.

A Covered Entity is one of the following:

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.

But What Does HIPAA Do?

HIPAA's intention is to provide a more standardized way to protect a patient's confidentiality and privacy while still allowing for care between a number of different healthcare providers and their business associates.

Privacy and Confidentiality

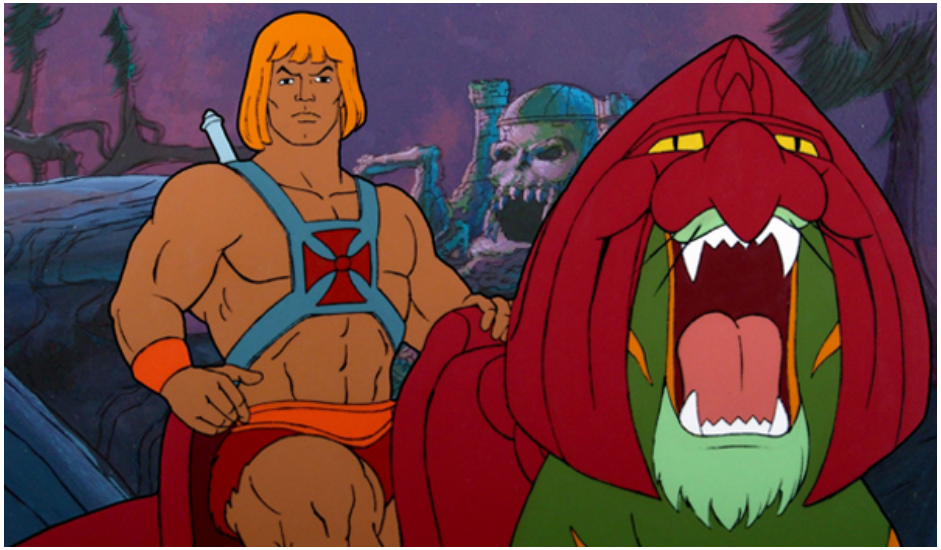
Patient information belongs to them(privacy)

Provider's owe patient's a duty to keep information confidential (confidentiality)

HIPAA Privacy and Confidentiality

- Every patient must be given a Notice of Privacy Practice (NPP) document. This describes how the organization will use and disclose a patient's medical information (replaces signed consent).

- Examples of what NPP typically covers: Treatment of patient, billing, obtaining payment from patient health plans, legally mandated reporting, and/or disclosure.



I HAVE THE POWER!!!!!

By the powers of HIPAA, patients have the power to control their personal health information.

HIPAA and PHI

- PHI or Protected Health Information refers to personal patient information that can be used to identify the patient, sometimes even inadvertently.
- HIPAA mandates patient control over this information.
- HIPAA allows patients to inspect their own medical records, correct errors, inquire who has access to their records and seek penalties if their medical information has been used inappropriately.

Examples of PHI

- Name
- Birth Date
- Fax Number
- Account Number
- Web Universal Resource Locator (URL)
- Street Address
- Admission Date
- Electronic mail address
- Certificate/License Number
- License Plate Number
- City
- Discharge Date
- Social Security Number, Vehicle and Serial Number
- Device Identifier and Serial Number
- Precinct
- Date of Death
- Medical Record Number
- Internet Protocol Number
- Full Face Photographic Images
- Zip Code
- Telephone Number
- Health Plan Beneficiary Number
- Biometrics Identifiers (i.e. finger prints)
- Any Other Unique Identifying Number, Characteristic, or Code

HIV/AIDS and HIPAA

- Confidentiality means that personal information is private, and may not be shared without the patient's permission. The confidentiality of a person's HIV status is important because people with HIV and AIDS face discrimination when other people find out they have HIV. People will only get tested and treated for HIV if they know their HIV status will be kept private.
- Federal and state laws require that a person's HIV status be kept confidential.

Copyright © 2010 R.J. Romero. www.hipaacartoons.com

"Someone reported there was P.H.I. in the dumpster."

HIPAA Situation

- In July 2013, Six workers at Cedars-Sinai Medical Center where Kim Kardashian gave birth were fired for snooping into her patient medical records.

(The Practical Guide to HIPAA Privacy by Rebecca Herold and Kevin Beaver; citing Los Angeles Times Nov. 2013)

HIPAA Enforcement

How is HIPAA Enforced?

- **The Public**. The public is increasingly educated about their privacy rights. They can take action by filing a claim with the federal Office For Civil Rights.
- **Office For Civil Rights (OCR).** If a covered entity or business associate violates the HIPAA rules, the Office for Civil Rights of the Department of Health and Human Services may investigate and impose civil and criminal penalties against the violating health care provider. **HIPAA does not provide a private cause of action to individuals affected by a health care privacy breach.** This means that an individual whose PHI has been used or disclosed by a health care provider in violation of HIPAA may not bring a civil claim against the health care provider under HIPAA.

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

How is HIPAA enforced?

- **Department of Justice (DOJ).** Agency involved in criminal privacy violations. Provides fines, penalties and imprisonment to offenders.

- **State Attorneys General:** The Health Information Technology for Clinical and Economic Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, gave State Attorneys General the authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules. The HITECH Act permits State Attorneys General to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules.

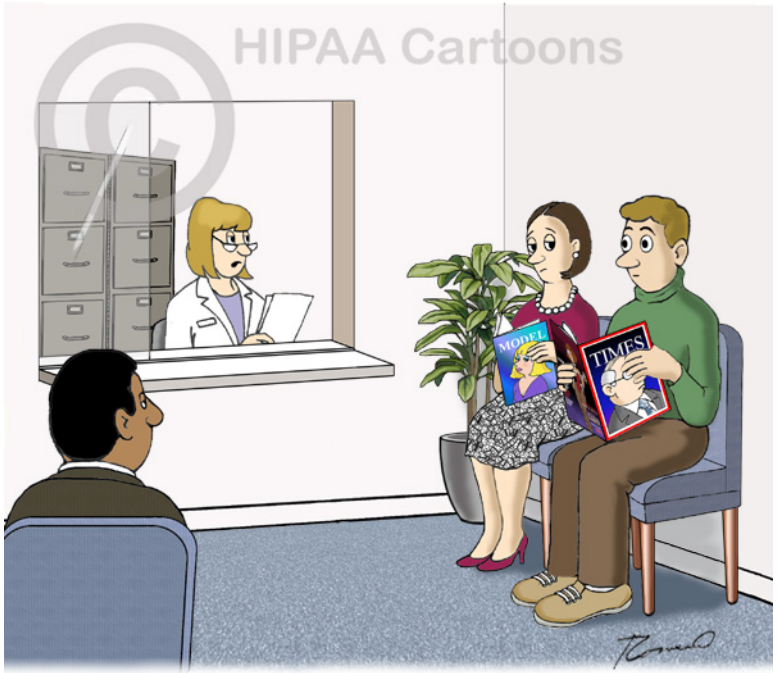
HIPAA Private Cause of Action

- HIPAA preempts any **contrary provision of state law**, meaning that a state law claim cannot be brought where a health care provider cannot comply with both the state and federal laws, or where the state law is an impediment to HIPAA's objectives.
- Recent decisions by state courts, however, have held that **HIPAA is the standard industry practice for health care providers and may form the basis for state law negligence claims involving disclosure of patient medical records.**

HIPAA Enforcement Penalties

- **Federal Government** protects PHI through HIPAA regulations:
  - Civil penalties up to $1,500,000/year for identical types of violations.
  - Criminal penalties:
    - $50,000 fine and 1 year prison for knowingly obtaining and wrongfully sharing information.
    - $100,000 fine and 5 years prison for obtaining and disclosing through false pretenses.
    - $250,000 fine and 10 years prison for obtaining and disclosing for commercial advantage, personal gain, or malicious harm.

HIPAA Meets the Real World: OCR Enforcement



"The doctor is running a bit late. So Mr. Kelly, how's that rash on your groin coming along?"

MOST FREQUENT ISSUES

- Impermissible uses and disclosures of PHI
- Lack of safeguards of PHI
- Lack of patient access to their PHI
- Uses or disclosures of more than the minimum necessary PHI
- Lack of administrative safeguards of electronic PHI

HIPAA Situation

- **State Hospital Sanctions Employees for Disclosing Patient's PHI**
  Covered Entity: Health Care Provider / General Hospital
  Issue: Impermissible Disclosure
- A nurse and an orderly at a state hospital discussed the HIV/AIDS status of a patient and the patient's spouse within earshot of other patients without making reasonable efforts to prevent the disclosure. Upon learning of the incident, the hospital placed both employees on leave; the orderly resigned his employment shortly thereafter. Among other actions taken to satisfactorily resolve this matter, the hospital took further disciplinary action with the nurse, which included: documenting the employee record with a memo of the incident; one year probation; referral for peer review; and further training on HIPAA Privacy. In addition to corrective action taken under the Privacy Rule, the state attorney general's office entered into a monetary settlement agreement with the patient.

HIPAA Situation

Large Provider Revises Patient Contact Process to Reflect Requests for Confidential Communications
Covered Entity: General Hospital
Issue: Impermissible Disclosure; Confidential Communications

- A patient alleged that a general hospital disclosed protected health information when a hospital staff person left a message on the patient's home phone answering machine, thereby failing to accommodate the patient's request that communications of PHI be made only through her mobile or work phones. In response, the hospital instituted a number of actions to achieve compliance with the Privacy Rule. To resolve this matter to the satisfaction of OCR, the hospital: retrained an entire Department with regard to the requirements of the Privacy Rule; provided additional specific training to staff members whose job duties included leaving messages for patients; and, revised the Department's patient privacy policy to clarify patient rights to accommodation of reasonable requests to receive communications of PHI by alternative means or at alternative locations

Minimum Necessary Requirement

The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is based on sound current practice that **protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.** The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

Minimum Necessary Requirement Exceptions

The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual's authorization.
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

HIPAA Situation

- **Dentist Revises Process to Safeguard Medical Alert PHI**
  Covered Entity: Health Care Provider
  Issue: Safeguards, **Minimum Necessary**
- An OCR investigation confirmed allegations that a dental practice flagged some of its medical records with a red sticker with the word "AIDS" on the outside cover, and that records were handled so that other patients and staff without need to know could read the sticker. When notified of the complaint filed with OCR, the dental practice immediately removed the red AIDS sticker from the complainant's file. To resolve this matter, OCR also required the practice to revise its policies and operating procedures and to move medical alert stickers to the inside cover of the records. Further, the covered entity's Privacy Officer and other representatives met with the patient and apologized, and followed the meeting with a written apology.

HIPAA Situation

- **Hospital Revises Email Distribution as a Result of a Disclosure to Persons Without a "Need to Know"**
  Covered Entity: General Hospital
  Issue: Impermissible Use and Disclosure
- A complainant, who was both a patient and an employee of the hospital, alleged that her protected health information (PHI) was impermissibly disclosed to her supervisor. OCR's investigation revealed that: the hospital distributed an Operating Room (OR) schedule to employees via email; the hospital's OR schedule contained information about the complainant's upcoming surgery. While the Privacy Rule may permit the disclosure of an OR schedule containing PHI, in this case, a hospital employee shared the OR scheduled with the complainant's supervisor, who was not part of the employee's treatment team, and did not need the information for payment, health care operations, or other permissible purposes. The hospital disciplined and retrained the employee who made the impermissible disclosure. Additionally, in order to prevent similar incidents, the hospital undertook a complete review of the distribution of the OR schedule. As a result of this review, the hospital revised the distribution of the OR schedule, limiting it to those who have "a need to know."

HIPAA Meets the Real World: Private Negligence Lawsuits using HIPAA

"Ok, I know you're still mad about that photo I took of your mother's medical procedure and posted to my Facebook wall. But to Tweet your friends about my hemorrhoids is violating my privacy."

HIPAA and State Negligence Claims

- **Emily Byrne v. Avery Center of Obstetrics and Gynecology, P.C. (Connecticut Case):**
- Ms. Byrne instructed the Avery Center not to release her medical information to the unborn child's father with whom she was no longer in a relationship. Under subpoena from the presumed father, the Avery Center released the information. The Avery Center did not inform Byrne or seek guidance from the Court on the extent of the disclosure to be made. **The Connecticut Supreme Court Ruled that a violation of HIPAA regulations may constitute a violation of generally accepted "standards of care," and remanded the case back to the lower court for trial.**

HIPAA and State Negligence Claims

- **I.S. v. Washington University (Missouri Case)**:
- I.S. was treated for colon cancer and requested that Washington University forward only the dates of the colon cancer treatment to her employer to satisfy company medical leave policies. Instead, Washington University forwarded I.S.'s employer a set of her medical records, including information regarding HIV status, mental health issues, and insomnia treatments. The Court allowed the state claim for negligence per se under HIPAA to stand.

HIPAA and State Negligence Claims

Hinchy v. WalGreen CO (Indiana Case):

- Abigail Hinchy had a sexual relationship and a child with Devion Peterson. Mr. Peterson was also carrying on a relationship with Audra Wither's, who was a pharmacist at WalGreen's. After Mr. Peterson discovered he had contracted genital herpes, he contacted Ms Wither's who then accessed Ms. Hinchy's prescription records at Walgreen's where she worked to determine if Ms. Hinchy had the disease. Ms. Withers discovered that Ms. Hinchy had not renewed her birth control pills during the time she became pregnant and she informed Mr. Peterson who then confronted Ms. Hinchy with the information via text explaining that he had a print out that proved she did not renew her birth control pills. After a jury trial, Ms. Hinchy was awarded 1.8 million dollars and Walgreen's and Ms. Withers were responsible for 80% of that amount.
- The appeals court upheld the amount of the verdict and the liability of Walgreens as the employer through the concept of vicarious liability which means the employer was held liable, not because the employer did anything wrong but because of their relationship with the wrongdoer.

HIPAA After the Breach

"Somehow your medical records got faxed to a complete stranger. He has no idea what's wrong with you either."

Breach Notification Rule

- The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

Breach Notification Rule

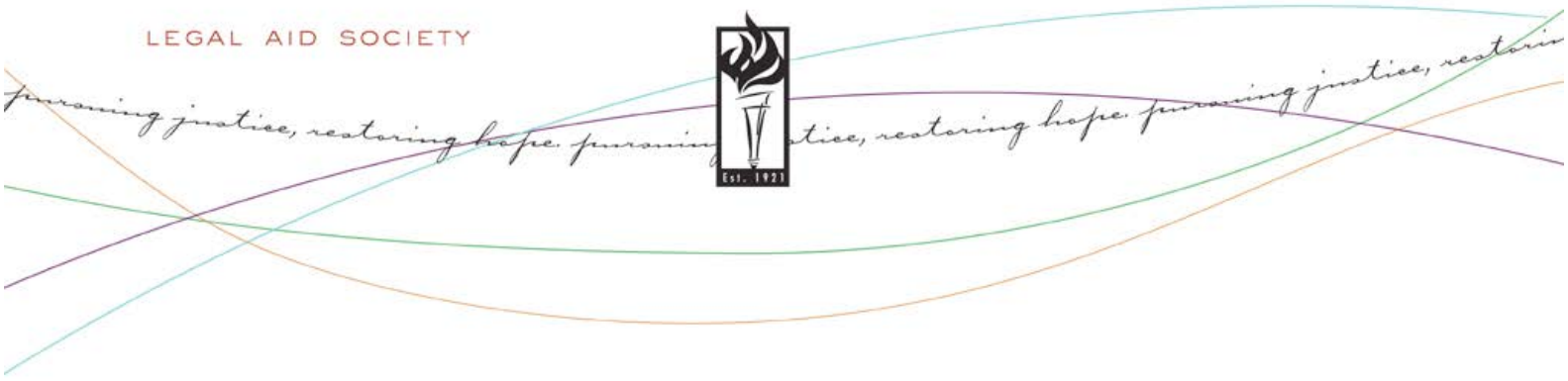
Definition of Breach (45 C.F.R. 164.402)

Impermissible use or disclosure of (unsecured) PHI is assumed to be a breach unless the covered entity or business associate, demonstrates a low probability that the PHI has been compromised based on a risk assessment.

Breach Notification Requirements

- Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

The End


LEGAL AID SOCIETY
pursuing justice, restoring hope.
Est. 1921