Basic Rights and Obligations of Consumers and Providers
What is HIPAA?

“No, it's not a female Hippopotamus, anyone else know?”
HIPAA

Health Insurance Portability and Accountability Act of 1996. Goal:

- Make it easier for people to keep health insurance
- Protect the confidentiality and security of healthcare information
- Help the healthcare industry control administrative costs
Who must comply with HIPAA?

- Covered Entities
  - Health plans
  - Healthcare clearinghouse
  - Healthcare providers that transmits any health information in electronic or other form in a transaction covered by HIPAA
Who must comply with HIPAA (cont.)?

- Business Associates
  - Consultants
  - Billing companies
  - Accountants
  - Lawyers
  - Accreditation agencies
  - Management companies
  - Business partners
  - Subcontractors
Who Need NOT comply with HIPAA?

Those who are not “covered entities,” such as:

- Life insurers
- Employers
- Workers’ compensation carriers
- Most schools and school districts
- Many state agencies (ex. DCS/CPS)
- Most law enforcement agencies
Main HIPAA Regulations

1) Standards related to the electronic transmission of healthcare information
   • Electronic transaction sets
   • Code sets
   • Unique identifiers

2) Procedures used to ensure the security and privacy of health information
   • Security of electronically stored data
   • Patient healthcare information privacy
The HIPAA Privacy Rule

Regardless of whether information is stored electronically or otherwise:

• Establishes national standards to protect individuals’ medical records and other protected health information.

• Requires appropriate safeguards to protect the privacy of PHI

• Sets limits and conditions on the uses and disclosures of PHI without authorization.

• It also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
The Privacy Rule in Arizona

Follows the HIPAA established standards and requirements

- Gives patients control of their records
- Set limits on use and disclosure
- Provides a balance between privacy protection and public responsibility
- Establishes accountability for violators

In Arizona, as well as most other states, the specific statues that have been adopted also allow for tort claims in certain situations.

In Arizona it is **A.R.S. § 36-509**
The Privacy Rule and Protected Health Information (PHI)

Protects all “individually identifiable health information”, or (PHI)

- PHI includes:
  - Oral or recorded information
  - Information on past, present, or future physical or mental health condition
  - All healthcare treatment
  - Past, present, or future payment for healthcare
  - Name, address, birth date, Social Security number
“According to your HIPAA release form I can’t share anything with you.”
So if everything is PHI, I should never share any information about a patient with anyone.

Wrong

Sharing information about a patient’s healthcare is often both appropriate and in the patient’s best interest.

Carelessness, of course, is not permitted.
A Note about A.R.S. § 36-509

Arizona Senate proposed SB1442 to make certain modifications to Arizona Statutes:

- A health care entity that acts in good faith under this article is not liable for damages in any civil action for the disclosure of records or payment records that is made pursuant to this article or as otherwise provided by law.

- The health care entity is presumed to have acted in good faith. This presumption may be rebutted by clear and convincing evidence.
A.R.S. § 36-509 and Disclosure to Family and Others

Proposed change specifically addresses disclosure of PHI by healthcare providers to:

“Persons, including family members, other relatives, close personal friends, or any other person identified by the patient, as authorized by or required by state or federal law.”

Takes certain factors into consideration, such as history of compliance, information received from family and others involved in patient’s treatment.
Remember – HIPAA is intended to **balance** privacy protection and public responsibility

PHI can be released when there is:

1. Patient consent/authorization to release information
2. One of the various exceptions applies
Patient Consent

Providers obtain patient consent before using or disclosing information for the purpose of providing treatment, related to payment for treatment, and healthcare operations.
Patient Consent Form

EXCEPTIONS

A signed consent is **NOT** needed, when:

- Provider has indirect relationship to the patient
- Care provided to incarcerated inmate
- Reasonable attempt was made to obtain written consent after emergency treatment
Patient Consent EXCEPTIONS (cont.)

- Consent is **NOT** required for:
  - Disclosures required by law
  - Victims of abuse, neglect, or DV
  - Warrants or court orders
  - Coroners, medical examiners, or funeral directors
  - Organ, eye, or tissue donations
  - Workers’ compensation compliance
  - Law enforcement to avert a serious threat to health or safety
  - Public health purposes and health oversight activities.
What about when Patients Want Access to their own Records?
Patients’ have a Right to Records under HIPAA

The Privacy Rules give patients the right to their own healthcare information.

- May inspect medical information
- May make copies of medical information
- May request corrections to medical information*
- May request a release of information or request restrictions on release
The Privacy Rules DO NOT give patients’ rights to control:

- Information compiled in anticipation of civil, criminal, or administrative actions or proceedings
- Information released for national security or intelligence reasons, or to law enforcement
- Certain health information that is subject to, or exempted from, the Clinical Laboratory Improvement Amendments (CLIA) of 1998
- Psychotherapy notes
Psychotherapy Notes include:

Notes recorded in any medium by a healthcare provider who is a mental health professional documenting or analyzing the contents of conversations during

- A private counseling session
- A group or joint counseling session
- A family counseling session

AND

- Are separated from the rest of the medical record
Psychotherapy Notes DO NOT include:

- Certain information that is not considered confidential communication
  - Medication prescription and monitoring
  - Counseling session start and stop times
  - Modalities and frequencies of treatment furnished
  - Results of clinical tests
  - Summary of the diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date
Psychotherapy Notes - Exceptions

May be used or disclosed without authorization:

• For a Covered Entity’s own training
• To defend itself against legal proceedings brought by the individual
• For Health and Human Services to investigate compliance with Privacy Rules
• To avert serious and imminent threat to public health or safety
• To a health oversight agency for monitoring
• For lawful activities by coroner or medical examiner or as required by law
General Exceptions to Disclosing PHI

- **De-identified information**
  - There are no restrictions on the use or disclosure of de-identified health information

- **Informal permission**
  - May ask the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object

- **In emergency situations**
  - Where individual is incapacitated or otherwise not available to consent
Catchall Exception to Disclosing PHI
Professional Judgment

Covered entities and providers generally may make such uses and disclosures of PHI, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

A.R.S. § 36-509 - “Persons, including family members, other relatives, close personal friends, or any other person identified by the patient, as authorized by or required by state or federal law.”

Takes certain factors into consideration, such as history of compliance, information received from family and others involved in patient’s treatment.
So why is everyone so afraid?

HIPAA and State statutes impose stiff penalties for violations – both civil and criminal.
Penalties for Violating HIPAA
No Private Right of Action

- Range from $100 - $50,000 for each violation
- Up to $1,500,000 for identical violations during a calendar year
- Considerations made for:
  - Nature and extent of violations
  - Nature and extent of harm resulting
  - History of prior compliance
- Statute of Limitations is 6 years
Penalties for Violating Related State Statutes

- Tort claims, including:
  - Negligence
  - Public disclosure of private facts
  - Invasion of privacy
  - Negligent Infliction of Emotional Distress
  - Intentional Infliction of Emotional Distress

- Statute of Limitations is 2 years (generally)
- Monetary damages can be in the millions
Special Note
Impact of the ACA on Adult Dependents

1) The Affordable Care Act has created a category of “adult dependents”* ages 18-26

2) Few states have laws to address adult dependents’ privacy

3) In 2013 California became first state to adopt a measure to ensure such privacy for this group

* adult dependents is not a defined term in the ACA
EXAMPLES

- Intentional disclosure of PHI to “uncovered entity”
- Unintentional disclosure of PHI to “uncovered entity”
Breach of Privacy Rule
Disclosure of PHI to “Uncovered” Entities

Intentional unauthorized release of PHI by provider

• Dental patient continuously asking for more pain medication.

• Dentist called patient’s’s employer to report a potential prescription pill addiction.

• Employee was subsequently demoted, and suffered significant decreased income

• Outcome: verdict for dentist*

Breach of Privacy Rule
Disclosure of PHI to “Uncovered” Entity

Intentional Unauthorized release - Vicarious Liability

• Hospital employee intentionally disclosed records to a patient’s boyfriend, who hospital employee knew personally

• Allegation of domestic violence was basis for hospital visit.

• Outcome: vicarious liability is available

Breach of Privacy Rule
Intentional Public Disclosure of PHI

Intentional Unauthorized release – Intentional Infliction of Emotional Distress

• Patient filed invasion of privacy against employee of health care provider following the Internet posting of information from patient's medical file re STD

• Intentional infliction of emotional distress also claimed

• Outcome: vicarious liability is available under certain circumstances.

Intentional Disclosure of PHI pursuant to Exception to Privacy Rule

- Patient and husband brought suit against physicians, employer, and hospital, alleging that privacy was invaded when bill with diagnosis of alcoholism was sent to employer.
- MSJ filed because employer was payor in this instance
- Outcome: Genuine issue of material fact exists for right to privacy claim.

Intentional Disclosure to those Involved in the Patient’s Care

- Area of enormous discussion – especially in Mental Health and Vulnerable Adult contexts
- Murphy Bill pushes for more sharing of information, especially with MH patients
- A.R.S. § 36-509 specifically allows it after considering specific factors:
  - Treatment history, including compliance
  - Necessary or useful in care compliance
  - Whether release would subject patient to DV, abuse or endangerment
Unintentional Disclosure of PHI

- Plaintiff underwent abortion and instructed that her home phone not be used for contact because she lived with parents.

- The NY Court ruled that punitive damages can be awarded for a grossly negligent breach of confidential medical information even if the breach was not intentional or malicious.

- Outcome: Verdict of $365,000 ($65,000 in compensatory emotional distress damages and $300,000 in punitive damages).
Special Note: Catchall Exception

Good Faith v. Professional Judgment

Covered entities and providers generally may make such uses and disclosures of PHI, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

BUT...
Good Faith and Professional Judgment

Good faith v. Professional Judgment and failure to disclose

- Private mental health hospital sued civilly for the murder of patient’s mother.
- The facility “had or should have had” knowledge that patient was likely to cause bodily harm to others if released from hospital; released patient without informing family or others of potential risk of harm.
- Hospital invoked “good faith” immunity standard.
- Outcome: Court found good faith must be based on “reasonable degree of care and skill” not mere independent good faith judgment.

BUT KEEP THIS IN PERSPECTIVE....

As of January 31, 2016:

• OCR has received over 127,184 HIPAA complaints (since 2003)

• Over 24,080 cases resolved by requiring changes in privacy practices, corrective actions, or providing technical assistance covered entities and their business associates (18%)

• In 10,943 cases, investigations found no violation had occurred. (8%)

• In 12,061 cases, OCR provided technical assistance to HIPAA covered entities, their business associates, and individuals without the need for an investigation. (9%)
PERSPECTIVE... (cont.)

• In the remaining 74,292 cases OCR determined the complaint was not eligible for enforcement (58%)

• Only 7% of cases reported resulted in enforcement beyond assistance and corrective action

• How many result in private action under State statutes has not been determined
In Summary:

Compliance with HIPAA requires covered entities to:

• Use and disclose information in accordance with HIPAA (and A.R.S. § 36-509 in Arizona)
• Adopt written policies for compliance
• Educate current and future employees about the rules and procedures
• Where procedures are lacking, establish policies and implement procedures to ensure security and privacy; self report when necessary
Comments, Questions, Suggestions
Thank You

ARTEMiS Law Firm
6424 E Greenway Parkway
Suite 100-383
Scottsdale, Arizona 85254
480-718-5890
ArtemisLawFirm.com

Victoria Ames, Esq.
VAmes@ArtemisLawFirm.com