The Basics and Beyond for Healthcare Providers
What is HIPAA?

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

Health Insurance Portability and Accountability Act of 1996

- Enacted by Congress in response to the rising costs of administrative expenses in healthcare, due largely to:
  - Complex coding systems
  - Lack of communication among providers about diagnostic and billing information
Goals of HIPAA

- 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. 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 Privacy Rule

- 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
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, then I should never share any information about a patient with anyone. Right?

Wrong

Sharing information about a patient’s healthcare is often both appropriate and in the patient’s best interest.
BUT... don’t be careless

- Hold Your Tongue!
  - When discussing Protected Health Info (PHI), consider your surroundings and speak quietly.
  - If you overhear or inadvertently come across PHI, be discreet and protective of this information.

- Check!
  - Double your service by double checking!
  - HIPAA regulations require us to safeguard a beneficiary’s Protected Health Info (PHI).
  - Always:
    - Double check the e-mail, postal address, or fax number before you transmit PHI.
    - Double check that you’re sending to the right person, not a general inbox.

- Is Your PHI Showing?
  - Don’t leave beneficiary records or other Protected Health Info (PHI) unattended on your desk.
  - Don’t leave it visible on your computer screen.
  - Lock your computer when leaving the area.
  - At the end of the day, lock all printed materials in a drawer or file. Log off your computer.

- Wrong address, wrong fax, and PHI? Oh My!
  - If you accidentally transmit Protected Health Info (PHI) to the wrong fax, e-mail or postal address:
    1. Immediately contact the incorrect address and have the PHI destroyed.
    2. Go to HIPAA. Complete an “Inadvertent Disclosure Form”;
    3. Submit the form to HIPAA’s HIPAA Privacy Officer.
  - Don’t send PHI to the wrong place!

Questions? Contact the HIPAA Privacy Hotline at 1-877-656.
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
Let’s Demystify the Myths and Misunderstandings about HIPAA privacy regarding:

- Consents
- Authorizations
- Releases of Information
- Patient Access to Records
- The Exceptions -- when Public Interest trumps Privacy
Consent vs. Authorization

CONSENT means consent to use PHI for treatment, payment, and healthcare operations

AUTHORIZATION means authorization use and disclose PHI not otherwise allowed by the rule (generally for a use other than treatment, payment, and healthcare operations)
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

Forms must:

- Contain clear language the average patient can easily understand
- Refer to the privacy notice and the right to change notice
- Advise the patient of his right to request restrictions on use/disclosure of PHI and provider’s right to deny request
- Advise of patient’s right to revoke consent in writing
- Be signed by patient
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 Refusal to Sign Consent Form

- If patient refuses to sign the consent to treatment form, a provider may refuse to provide treatment and explain why to patient.
- If patient continues to refuse to sign, provider must:
  - Send patient letter, preferably by certified mail, explaining why treatment withheld
  - Provide patient with list of alternative healthcare resources
  - Clearly document these transactions in the patient’s file
Patient Authorization

Providers must obtain patient authorization before using or disclosing private healthcare information for purposes other than treatment, payment, or healthcare operations – like marketing, advertising, research, etc.
Patient Authorization Form

Form must state:

• An easily understandable description of information to be used/disclosed
• A clear identification of the person or class of persons authorized to use it
• An expiration date or event
• That the patient has a right to revoke authorization at any time
• That the information may be subject to re-disclosure by recipient and no longer protected
Patient Authorization Form (cont.)

Form must (cont.):

- State that provider cannot condition treatment of signing form
- That patient may refuse to sign form
- Include a description of the purpose of each requested use or disclosure
- Include patient or representative signature and date
- Whether doctor or provider will be paid (for research or marketing activities)
Form 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.
Release of Information

This is just another name for a patient authorization.

Often called an authorization to release information
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 or information or request restrictions on release
Patients’ Right to Records

EXCEPTIONS

The Privacy Rules DO NOT give patients’ rights to control the following:

• 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.
So why is everyone so afraid?

HIPAA imposes stiff penalties for violations – both civil and criminal
Penalties for Violating HIPAA

- 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
Privacy Rule Compliance

Compliance with HIPAA requires providers to:

• Use and disclose information in accordance with HIPAA
• Adopt a written privacy policy
• Educate current and future employees about the privacy procedures
• Where privacy procedures are lacking, establish policies and implement procedures to ensure privacy and security
Key points to remember

- Keep the best interest of your patient at the forefront
- Seek authorization for release of PHI when required
- Document your discussions and disclosures
- Consult with your in-house or private legal counsel when in doubt
Comments, Questions, Suggestions
Thank You

14901 N Scottsdale Road, Suite 302
Scottsdale, Arizona 85254
480-718-5890
ArtemisLawFirm.com

Victoria Ames, Esq.
VAmes@ArtemisLawFirm.com