Compliance with HIPAA
In 1996 the Health Insurance Portability and Accountability Act was passed by the federal government. Its primary aim was to force health care providers to protect the privacy of patient health information (PHI).
HIPAA

- Federal law
  - Mandates industry-wide standards for health care information on electronic billing and other processes
  - Requires the protection and confidential handling of protected health information
- Privacy and Security Rule
- Generally applies to **Covered Entities** and **Protected Health Information**
Hybrid Entity

What Is a hybrid entity?
• A hybrid entity under HIPAA is a single, legal, covered entity whose business activities include both covered and non-covered functions and that designates certain units as health care components.

What is a covered entity?
• Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.

What are we?
• Texas A&M University is a hybrid entity
HIPAA: Protected Health Information (PHI)

Definition:
Individually identifiable health information from a covered entity in any form (paper, oral, electronic) that relates to:

1) The health status or condition of an individual;
2) Provision of health care to an individual; or
3) Payment for provision of health care to an individual
To simplify, PHI:

- Comes from a covered entity and is any information that can identify or potentially identify a patient and/or pertains to the patient's past, present or future health status.

For us this is:

- Name, DOB, SS#, history, meds, chief complaint, etc.
Restricted Use and Disclosure of PHI

• Patients can ask that health information not be shared with certain people, groups, or companies. In cases like this, you will need to make your supervisor aware of this request as soon as possible.

• For example, a patient may ask that their information not be shared or made known to a certain member of their family.
When is it okay to release PHI?

- Generally patients must give a covered entity WRITTEN consent to release any PHI.
- PHI can be released on a person deceased for more than 50 years.
- PHI can be given to the patient’s guardian, durable power of attorney for healthcare, or next of kin (if the patient is incapacitated).
- For operations (ex. quality assurance, incident reports, teaching and education of residents and students).
- To enable our organization to get paid for services rendered.
- When there is a legal duty to report (ex. child abuse, domestic violence, gunshot or stab wounds).
- It can be given to another healthcare provider who has treated the patient to enable that provider to get paid for their services.
What do you need to know?

HIPAA requires you to use the minimum amount of patient information needed to do your job efficiently and effectively.

Ask yourself:

• Do I need this information to do my job?
• What is the least amount of information I need to do my job?
When is it NOT permissible to disclose PHI?

Posting it on Social Media

- You may not post details about patients on any electronic medium. This is true even when a patient’s name is not used. If there is enough information for someone to identify the patient (for example the nature of the injury, the time and location of an incident, etc.) the provider will be in violation.
When is it NOT permissible to disclose PHI?

Discussions with colleagues/friends

• Just as with electronic mediums, discussing patient encounters with colleagues who were not part of the patient care team (face to face, or in writing) is a definite no.

• This applies also to conversations outside of work with friends or family.

KEEP IN MIND: YOU NEVER KNOW WHO KNOWS WHOM!
When is it NOT permissible to disclose PHI?

Statements to news media

• You may not provide any information about the nature or severity of a patient’s illness or injuries.

• You may not verify the identity of a patient being treated EVEN IF the media agency claims to already know the identity of the patient.

“NO COMMENT” and/or “PLEASE SEE THE “Privacy Officer” are always rules of thumb!
When is it NOT permissible to disclose PHI?

Sharing patient status or information with neighbors

• You may not disclose any patient information to a patient’s neighbor, friends, or other persons who are not involved in the treatment of said patient.

• If a concerned neighbor or friend wants to know about the patient, let the patient tell them.
SECURITY

• Print-based medical records need to be kept in a secure area or in a safe location with access by authorized people only. (These areas should be locked when not in use.)

• Access to those locations needs to be controlled so that we can maintain the security of records containing PHI.

• If you use a workstation as part of your job, a password (not to be shared) should be used to control access to PHI.

• If a workstation is available/viewable by nonauthorized people, use a screensaver or reposition the screen to protect the viewing of PHI.

• Lock cabinets that contain PHI when you leave your area.
Why is HIPAA Important?

• Individuals and agencies who violate HIPAA privacy can be fined and individuals can even serve jail time if found guilty of violating these statutes.

• It’s just the right thing to do – we are patient advocates and should be protecting the privacy of our patients.
HIPAA: Key Rights

The rights of patients under HIPAA:

- Permit or refuse to permit disclosure of PHI when permission is required
- Receive Notice of privacy practices
- Access and obtain copies of PHI
- Receive an accounting of how PHI has been disclosed outside normal patient care channels
- Seek amendment/correction to PHI
HIPAA Disclosure Notification

• In the event that PHI is accidently or deliberately disclosed in violation of HIPAA regulations, the covered entity is required to report the disclosure immediately.

• It is unlawful to hide or cover-up any confirmed or potential disclosure.

• If you feel that a HIPAA disclosure has occurred, report the situation to the TAMU Privacy Officer immediately!
HIPAA: Penalties

- Enforcement is by the Office of Civil Rights (OCR), a division of the United States Department of Health and Human Services (HHS)

- HIPAA has both criminal and civil penalties for individuals and companies.

  - Criminal penalties are generally reserved for the intentional unauthorized use, or disclosure of PHI, and consist of prison time and fines.

  - Civil penalties require no bad intent, and consist of fines
# Civil HIPAA breach penalties

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknowing</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>Willful neglect but violation is corrected within the required time period</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>Willful neglect and is not corrected within required time period</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>
Criminal HIPAA breach penalties

• Criminal violations of HIPAA are handled by the DOJ. As with the HIPAA civil penalties, there are different levels of severity for criminal violations.

• Covered entities and specified individuals, as explained below, who "knowingly" obtain or disclose individually identifiable health information, in violation of the Administrative Simplification Regulations, face a fine of up to $50,000, as well as imprisonment up to 1 year.

• Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to 5 years in prison.

• Finally, offenses committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000 and imprisonment up to 10 years.
END

John Pryde | Privacy Officer
Texas A&M University
Office of University Risk, Ethics, & Compliance
Jack K. Williams Administration Building, Suite 302
College Station, TX 77843

ph: (979) 845-9853
j pryde@tamu.edu