HIPAA and Privacy Quick Reference

Guidelines and Tips for Securing Information

Privacy and HIPAA

- **What is Privacy?**
  - Privacy is the fundamental right to be free from unauthorized intrusion.
  - Fundamental privacy rights include the right to
    - Access your own records.
    - Correct your own records.
    - Limit the types of information shared from your record.
    - Limit who can access your record.
    - File a complaint.
  - The United States has a multitude of privacy laws covering personal privacy, healthcare, education, safety, etc.
  - States also have privacy laws that mirror or augment individual federal privacy law.
- **HIPAA**
  - HIPAA is federal legislation protecting the privacy and security of patients' health information.
  - The Texas Medical Records Privacy Act mirrors HIPAA and expand its applicability to any individual possessing PHI.
- **HIPAA Rights – You Have the Right to:**
  - Your Records
    - Obtain an electronic or paper copy of your medical record.
    - Ask provider to correct your medical record.
  - Confidentiality
    - Request the provider communicate confidentially with you.
  - Information Sharing Limits
    - Ask the provider to limit what information they use or share about you.
    - Ask the provider to share information with specific family, friends, or others.
    - Receive a list of everyone with whom the provider has shared your information.
  - Privacy Notice
    - Receive a copy of the privacy notice explaining your rights.
  - Personal Representation
    - Choose someone to act on your behalf.
  - File a Complaint
    - File a complaint if you feel your rights have been violated.

PII and PHI: What Needs Protecting?

- **Personally Identifiable Information (PII)**
  - PII is any information connected to a specific individual which can be used to identify the individual directly or indirectly.
  - PII can include:
    - Demographics
    - Personal ID numbers (SSN, DL number, etc.)
    - Physical email address,
    - Personal characteristics (biometrics, pictures, etc.)
- **Protected Health Information (PHI)**
  - PHI includes all individually identifiable health information relating to an individual's:
    - physical or mental condition
    - health care services received, or
    - payment for health care received
  - PHI Identifiers
    - Identifiers of an individual or their relatives, employers, or household members are protected

under HIPAA. The combination of these elements cannot be used to re-identify the individual:

- ✓ Telephone number
- ✓ Fax Number
- ✓ Email address
- ✓ SSN
- ✓ Medical record numbers
- ✓ Health Plan beneficiary number
- ✓ Account number
- ✓ License/Certificate number
- ✓ VIN/Serial/License Plate numbers
- ✓ Device identifiers or serial numbers (for pacemaker, medical implants, etc.)
- ✓ URL
- ✓ IP address
- ✓ Biometrics (fingerprint, voice print, etc.)
- ✓ Full face photographs
- ✓ Tattoos and scars
- ✓ Any other unique identifying number, characteristic or code.

❖ **Who Needs to Comply**

- ➢ All Travis County employees and contractors are responsible for keeping PII and PHI safeguarded from loss and unauthorized changes or exposure.

Minimum Necessary: How Much Do I Really Need?

❖ **Minimum Necessary**

- ➢ The Minimum Necessary Standard states that the amount of information shared should be the least amount needed to fulfill a request. This is to help protect patient privacy.
- ➢ When sharing or requesting a patient's health information, consider what is really needed to complete the task – and what is not.
- ➢ Before responding to a record request, carefully consider what information the requestor really needs for their purposes.

Consent and Authorization

❖ **Consent**

- ➢ Generally, no patient health information should be shared unless the patient has expressly given their consent. This applies to
  - ▪ whom their information can be shared with.
  - ▪ the specific type of information that can be shared.
  - ▪ the format by which it is shared (email, voicemail, phone, etc.).

❖ **Authorization**

- ➢ Anyone with whom you share a patient's medical information must
  - ▪ have a legitimate need for it, and
  - ▪ be authorized to receive it.
- ➢ Even when sharing within Travis County. Whether sharing from one Department to another or between coworkers in the same division, the recipient

must have a proper business need, authorization to access the information, and consent from the patient to receive such information.

- If you are unsure whether a piece of information can be shared, always contact your Travis County Compliance and Privacy Office for guidance.

Civil and Criminal Penalties

- **Penalty**
  - Each person in an organization is responsible for security. Similarly individuals can be held liable and penalized for damages resulting from privacy failures.
  - The penalties for HIPAA violations include civil monetary penalties assigned by the federal Office of Civil Rights ranging from $137 to $68,928 per violation, depending on the level of culpability.
  - Violations can be assessed for each record involved.
  - Criminal penalties can also be imposed for intentional violations, leading to fines and potential imprisonment.

These penalties can be charged against the organization and against you personally.

Department of Justice Penalties for HIPAA Violations

Offense	Monetary Penalty	Prison Term
For certain offenses such as knowingly obtaining PHI	Up to $50,000 AND	Up to 1 year
If the offenses are committed under false pretenses	Up to $100,000 AND	Up to 5 years
If the offenses are committed with the intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm	Up to $25,000 AND	Up to 10 years

Snooping – Mind Your Business

- **Snooping**
  - Snooping is an attempt to learn information that is not intended to be visible or shared. Someone snooping typically does not have authorization to access the person's information being targeted.
  - People who are tempted to snoop could be a client's family members, partners or ex-partners, members of the media who are curious about someone's condition, and many others. That curiosity may be from genuine concern or from general nosiness.

Neither overrules someone's right to privacy.

- HIPAA rules expressly require that anyone accessing a client's PHI must have
  - A legitimate business reason for accessing the information, and
  - Authorization – either from the client or by

virtue of their healthcare relationship - to receive the information. ➢ HIPAA rules also require that even those authorized to access information only obtain the minimum	amount of information needed for their purposes. Any additional information accessed would be considered snooping and possibly an unauthorized access of information,	which could result in penalties.