Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that establishes standard privacy protections for Protected Health Information (PHI). Also known as the "Privacy Rule" these regulations respond to patient's concerns about the privacy of their health information and establishes specific patient rights regarding the use and disclosure of this information.

Protected Health Information (PHI) is patient information in any form (oral, written, or electronic) that has at least one item that identifies a patient, such as any of the following:

- Name
- Dates of (birth, death, etc)
- Address (all geographic subdivisions smaller than state)
- Telephone or fax number
- Email address
- Social security number
- Medical record number
- Health Plan beneficiary number
- Account number
- Biometric identifiers
- Certificate/license numbers
- Device identifier or serial number
- Web address/IP address
- Photographic images
- Vehicle or drivers license numbers
- Any other characteristic that could uniquely identify the person

Protected Health Information (PHI) includes patient medical records but includes other kinds of patient records. It also includes, for example:

- An oral conversation where you talk to someone not involved in a patient's care and identify the patient. For example, you say something like this: "Jane Doe is very sick with chicken pox."
- Fax information where a social security number and other health information is shared
- Patient care billing information
- Emails and text messages that include patient information
- Schedules of medical appointments
- Photographs of patients

Protected Health Information (PHI) can be accessed and shared if:

- It is for treatment, payment, or UTRGV School of Medicine's healthcare operations
- It is required by law (such as required reporting of child or elder abuse/neglect, required reporting of communicable diseases, and responding to court orders)

- UTRGV receives a signed permission form (known as an "authorization form") by the patient or in some circumstances, a patient's parent or legal guardian

Your access to Protected Health Information (PHI) should be based on your job function

- A health professional may share PHI with another health professional if the person has a treatment relationship with the patient and it is for treatment purposes
- Individuals not involved in treatment (e.g., billing, quality improvement and credentialing personnel) must limit their access and disclosure of PHI to the minimum necessary to perform their job functions.

Minimum Necessary Rule

An important aspect of the HIPAA Privacy Rule is the principle of "minimum necessary". UTRGV employees must make reasonable efforts to request, use, and share only the minimum amount of PHI needed to accomplish the intended purpose. When the minimum necessary standard applies to a use or disclosure of PHI, employees may not request the entire medical record for a particular purpose, unless this purpose specifically justifies the whole record as the amount reasonably needed to accomplish the intended purpose.

The minimum necessary requirement does not apply to:

- Health care providers for treatment purposes
- Disclosures to the patient or their legal representative
- Disclosures made in accordance with an authorization
- Other disclosures required by law

Patient information used in research is subject to special HIPAA provisions. Please contact the Institutional Review Board (IRB) for more information at 956-665-2093

Sharing PHI with a Patient's Family and Friends

In a patient care setting you may, but are not required to, disclose Protected Health Information (PHI) to a patient's friends or family members who are involved in the patient's care or payment for their care, but only in specific circumstances. They are:

- If a patient agrees, you may disclose Protected Health Information (PHI) to a family member or a friend.
- If it is an emergency situation or the patient is unable to communicate, a healthcare provider may use his or her professional judgment to disclose only relevant or limited Protected Health Information (PHI) to a friend or family member.
- If the patient is a minor or has a legal guardian, you may disclose Protected Health Information (PHI) only to the parent or legal guardian, and if the parent or legal guardian gives you permission to disclose PHI then you may communicate with other family members or friends

If the patient does not agree, then you may not disclose Protected Health Information (PHI) to friends or family members even if the patient is deceased.

For example:

- A surgeon may not discuss the results of a surgical case with family, friends or visitors who are not authorized by the patient to receive Protected Health Information (PHI).

- A provider may not discuss the patient's HIV status, drug use, pregnancy, or any other sensitive information in front of family, friends or visitors unless authorized by the patient.

HIPAA Violations

Employees are expected to prevent HIPAA violations that are within their direct control. For example:

- Accessing a medical record of a friend or family member to see how they are doing;
- Gossiping to neighbors or others about patients;
- Talking loudly in open areas about patients or family members;
- Keeping paper records open so that anyone can see them;
- Writing information about patients or other health information on Facebook, Twitter or other social networking sites;
- Taking pictures of patients and family members in the hospital with your cell phone or other device, without specific oversight or proper written permission;
- Writing emails which contain patient information to people who do not need to know;
- Accessing medical records to find information to use in employment decisions, such as hiring decisions, verifying why employees were absent, etc.
- Selling patient information; and
- Disclosing Protected Health Information (PHI) at a place of worship.

Employees are also expected to avoid exposing Protected Health Information (PHI) to HIPAA violations by others. For example:

- Allowing others to use their passwords or other authentication information to access systems containing Protected Health Information (PHI);
- Copying Protected Health Information (PHI) onto thumbdrives, laptops, or other electronic medium that are not encrypted according to University standards;
- Leaving documents with Protected Health Information (PHI) in unlocked cars and other unprotected places; and
- Disposing of documents with Protected Health Information (PHI) without shredding them first.

All HIPAA violations must be reported to the Privacy Officer, Diane Sheppard, at 956-296-1424 as soon as possible. This step is essential to ensure that UTRGV responds to all violations in a timely manner in accordance with specific HIPAA requirements.

Protecting PHI

Everyone must make reasonable efforts to safeguard patient information and avoid prohibited uses and disclosures of Protected Health Information (PHI).

How Can I Protect Written PHI?

Written PHI is Protected by:

- Turning over and covering up notes in common areas.

- Shredding paper containing patient information or placing paper in shredding bins, when appropriate.
- Remove Protected Health Information (PHI) from conference rooms, copiers/FAX machines, library, and other locations after use.
- White boards or care logistics boards should display minimal identifiable patient information.
- Patient charts should not be visible to the public. Store charts or documents with the patient name covered, turned over, or in a wall bin with name facing the wall.
- Ensuring that paper files are in a locked and secure area. Do not leave them in a car.
- Keeping fax machines used to transmit or receive Protected Health Information (PHI) in a monitored and secure area.
- Confirming with the intended recipient the mailing address, fax number, or email address before sending Protected Health Information (PHI).

Note: Protected Health Information (PHI) known to be sent or received by the wrong person by fax, mail or email must be reported to the Privacy Office immediately.

How Can I Protect Oral PHI?

Oral PHI is Protected by:

- Quietly discussing patient issues so that others cannot overhear.
- Avoiding conversations about patients and their identifying information in public places such as an elevator, hallway, or lunchroom.
- Conducting walking rounds in lowered voices, whenever possible.
- Closing exam room doors during consultations or treatment of patients.
- Keeping overhead pages to a minimum and not including treatment information on these pages.
- Conducting end-of-shift reports, telephone conversations, and dictation in a private location, whenever possible.
- Limiting access to patient areas, ensuring that the area is supervised, and escorting non-employees in the area.

How Can I Protect Electronic PHI?

Electronic PHI is Protected by:

- Never share your password with anyone.
- Use strong password that includes symbols such as +*&%!#$" according to UTRGV Information Security Standards.
- Never disclose or share Electronic Protected Health Information (ePHI) on any social networking site. Social networking sites can include Facebook, Caringbridge, and Twitter. Less obvious, but still considered social networking sites are blogs, forums, and YouTube.
- Never send, forward or auto-forward Electronic Protected Health Information (ePHI) or confidential information to your personal email account or unapproved 3rd parties such as Gmail, AOL, Yahoo, Google Docs, or Dropbox.

- Never take pictures, recordings, or videos of patients, without permission.
- Use extra caution when downloading programs from the Internet to your computer.
- When sending email outside of UTRGV clinics, such as to another hospital or insurance company, send only through SecureMail. To do this, type [secure] at the beginning of the subject field of your email. Note that square brackets are used. For Example:
    - Subject: [secure] Monthly Report
- Store portable electronic media or computers in a physically secure location (locked cabinet, desk, office, etc.). Do not leave them visible in your car or in a public area where they could be stolen or lost;
- Use screen savers or privacy screens when computer screens are clearly visible to others;
- Never store or share Electronic Protected Health Information (ePHI) on any unencrypted devices (usb, laptop, etc.), including unencrypted personal computers and devices; and
- Store all electronic files that contain Electronic Protected Health Information (ePHI) and confidential information on your department's network drive.

HIPAA Patient Rights

In addition to regulating Protected Health Information (PHI), HIPAA gives patients ten specific rights:

1. Notice of Privacy Practices - UTRGV clinics must provide a Notice of Privacy Practices no later than the first clinical encounter. In addition, all UTRGV clinics must post the notice at each clinical site in a clear and prominent place. UTRGV clinics must make a good faith effort to obtain written acknowledgement from patients of receipt of the notice.

2. Patients may ask to see a copy of their medical records and billing records and/or completed test results in a format they request, such as a paper or electronic copy.

3. Patients may request that a copy of their health information be transmitted directly to another person that they have designated with a signed authorization.

4. Patients may request changes to their health record if the information is not correct or complete. This is known as an amendment request.

5. Patients may request restrictions or limitations on how their health information is used or released.

6. Patients may request that their health information not be disclosed to their health plan for a health care item or service which they or a family member pays in full.

7. Patients may decide if they want to give their permission before their health information can be used or shared for certain purposes, such as for marketing or fundraising (known as an "Authorization").

8. Patients may receive a report on when and why their health information was shared for certain purposes (known as an "Accounting of Disclosures").

9. Patients may receive confidential communications (such as medical records, billing, etc.) by an alternative means or location such as an alternative address, for example a PO Box, rather than their home address.

10. Patients may file a complaint, if they believe their rights were denied or their health information was not protected. Complaints may be filed with the Privacy Office, the Office for Civil Rights US Department of Health and Human Services, or the Texas Department of State Health Services.

Responding to Privacy Complaints from Patients

UTRGV School of Medicine takes patient privacy seriously. We listen and respond to the concerns and complaints of our patients. A patient will not be denied access to care or discriminated against for filing a complaint. It is important that we take all patient complaints seriously and know how to assist a patient wanting to file a complaint. In many cases, a privacy complaint may actually be a request to exercise one of the 10 patient's rights. Contact your supervisor or the Privacy Officer for assistance in responding to complaints from patients.

What Happens to Violators at UTRGV School of Medicine?

UTRGV School of Medicine employees may face disciplinary action for violating the Health Insurance Portability and Accountability Act (HIPAA) and/or UTRGV School of Medicine policies. This disciplinary action may include:

- Additional Training
- Oral Warning
- Written Counseling
- Probation
- Suspension
- Termination

In addition to disciplinary action, an employee could face civil and criminal penalties.

Your HIPAA Responsibilities

First and foremost, you are responsible for complying with HIPAA. Compliance with the provisions of HIPAA includes:

- Protect and safeguard patient information.
- Notify the Privacy Office of any privacy complaint or concern and/or the Information Security Office for any security complaint or incident or if there has been a loss or theft of Protected Health Information (PHI) or confidential information.

A breach would include a lost or stolen laptop, cell phone, USB stick or paper records. A breach could also be an attack of computer viruses or hackers into our information systems, or emails or fax information sent to the wrong place. Employees are expected to report suspected or confirmed privacy violations. To report a privacy violation, contact the Privacy Office.

Our HIPAA Responsibilities – Protection from Retaliation

Any employee who becomes aware of, or experiences any type of retaliation for reporting suspected privacy violations, or for assisting in privacy-related investigations should immediately report such acts by following HOP ADM 4-301 Non-Retaliation , or by contacting the Privacy Officer. Acts of retaliation can take on many forms, including but not limited to: intimidation, threats, coercion, discrimination, harassment, demotion and/or termination.

The Compliance Office can be reached at the Compliance Hotline (Toll Free) at (877)882-3999 or email http://www.utrgv.edu/compliance/

I hereby acknowledge that I have attended the HIPAA orientation provided by the UTRGV School of Medicine IT department. I also acknowledge that I have received and read the HIPAA policy and I understand and agree that my use of University Information Resources for patient information is conditioned upon my agreement to comply with the HIPAA Policy and that my failure to comply with this Policy may result in disciplinary action up to and including termination of my employment.

Signature: _____ Date: _____

Print Name: _____