Athena New User Access Request - Med Student

Please fill out this form in order to be considered for UTRGV EMR access. Your request will be responded to as soon as possible. Please list your name as it is shown on your Government ID.
***Please note that it may take up to 2 business days for new user requests to be processed.*

Full Name:_____ DOB:_____

UTRGV Email:_____ Student ID:_____

Phone:_____

Medical Student ◯ 1st Year ◯ 2nd Year ◯ 3rd Year ◯ 4th Year

The University of Texas Rio Grande Valley

INFORMATION RESOURCES ACCEPTABLE USE AND SECURITY POLICY AGREEMENT

All individuals granted access to or use of System Information Resources must be aware of and agree to abide by the following acceptable use requirements:

Definitions	• **University:** The University of Texas Rio Grande Valley • **System**: The University of Texas System. • **University Information Resources**: All computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf. • **University Data:** All data or information held on behalf of University, created as result and/or in support of University business, or residing on University Information Resources, including paper records. • **Confidential Data or Confidential Information:** All University Data that is required to be maintained as private or confidential by applicable law. • **User:** Any individual granted access to University Information Resources.
General	• University Information Resources are provided for the purpose of conducting the business of University and/or System. However, Users are permitted to use University Information Resources for use that is incidental to the User's official duties to University or System (Incidental Use) as permitted by this policy. • Users have no expectation of privacy regarding any University Data residing on University owned computers, servers, or other information resources owned by, or held on behalf, of University. University may access and monitor its Information Resources for any purpose consistent with University's duties and/or mission without notice. • Users have no expectation of privacy regarding any University Data residing on personally owned devices, regardless of why the Data was placed on the personal device. • All Users must comply with applicable University and System Information Resources Use and Security policies at all times. • Users shall never use University Information Resources to deprive access to individuals otherwise entitled to access University Information, to circumvent University computer security measures; or, in any way that is contrary to the University's mission(s) or applicable law. • Use of University Information Resources to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the User's official duties as an employee of University and is approved in writing by the President or a specific designee. Viewing, access to, or storage or transmission of sexually explicit materials as Incidental Use is prohibited. • Users must clearly convey that the contents of any email messages or social media posts that are the result of Incidental Use are not provided on behalf of the University and do not express the opinion or position of University. An example of an adequate disclaimer is: "The opinions expressed are my own, and not necessarily those of my employer, The University of Texas Rio Grande Valley." • Users should report misuse of University Information Resources or violations of this policy to their supervisors.
Confidentiality & Security of Data	• Users shall access University Data only to conduct University business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access. Users shall maintain all records containing University data in accordance with University's Records Retention Policy and Records Management Guidelines. • Users shall not disclose Confidential Data except as permitted or required by law and only as part of their official University duties. • Whenever feasible, Users shall store Confidential Information or other information essential to the mission of University on a centrally managed server, rather than a local hard drive or portable device. • In cases when a User must create or store Confidential or essential University Data on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smart phone, the User must ensure the data is encrypted in accordance with University, System's and any other applicable requirements.

	• The following University Data must be encrypted during transmission over an unsecured network: Social Security Numbers; personally identifiable Medical and Medical Payment information; Driver's License Numbers and other government issued identification numbers; Education Records subject to the Family Educational Rights & Privacy Act (FERPA); credit card or debit card numbers, plus any required code or PIN that would permit access to an individual's financial accounts; bank routing numbers; and other University Data about an individual likely to expose the individual to identity theft. Email sent to and received from System and U. T. System institutions using University and/or System provided email accounts is automatically encrypted. The Office of Information Technology [or other applicable office] will provide tools and processes for Users to send encrypted data over unsecured networks to and from other locations. • Users who store University Data using commercial cloud services must use services provided or sanctioned by University, rather than personally obtained cloud services. • Users must not use security programs or utilities except as such programs are required to perform their official duties on behalf of University. • All computers connecting to a University's network must run security software prescribed by the Information Security Officer as necessary to properly secure University Resources. • Devices determined by University to lack required security software or to otherwise pose a threat to University Information Resources may be immediately disconnected by the University from a University network without notice.
Email	• Emails sent or received by Users in the course of conducting University business are University Data that are subject to state records retention and security requirements. • Users are to use University provided email accounts, rather than personal email accounts, for conducting University business. • The following email activities are prohibited when using a University provided email account: o Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work related purpose. o Accessing the content of another User's email account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the User's official duties on behalf of University. o Sending or forwarding any email that is suspected by the User to contain computer viruses. o Any Incidental Use prohibited by this policy. o Any use prohibited by applicable University or System policy.
Incidental Use of Information Resources	• Incidental Use of University Information Resources must not interfere with User's performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University or System policy. • Users must understand that they have no expectation of privacy in any personal information stored by a User on a System Information Resource, including University email accounts. • A User's incidental personal use of Information Resources does not extend to the User's family members or others regardless of where the Information Resource is physically located. • Incidental Use to conduct or promote the User's outside employment, including self-employment, is prohibited. • Incidental Use for purposes of political lobbying or campaigning is prohibited. • Storage of any email messages, voice messages, files, or documents created as Incidental Use by a User must be nominal (less than 5% of a User's allocated mailbox space). • Files not related to System business may not be stored on network file servers.
Additional Requirements for Portable and Remote Computing	• All electronic devices including personal computers, smart phones or other devices used to access, create or store University Information Resources, including email, must be password protected in accordance with University requirements, and passwords must be changed whenever there is suspicion that the password has been compromised. • University Data created or stored on a User's personal computers, smart phones or other devices, or in data bases that are not part of University's Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to University Information Resources • University issued mobile computing devices must be encrypted. • Any personally owned computing devices on which Confidential University Data is stored or created must be encrypted. • University Data created and/or stored on personal computers, other devices and/or non-University data bases should be transferred to University Information Resources as soon as feasible.

	• Unattended portable computers, smart phones and other computing devices must be physically secured. • All remote access to networks owned or managed by University or System must be accomplished using a remote access method approved by the University or System, as applicable.
Password Management	• University issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone. • Each User is responsible for all activities conducted using the User's password or other credentials.

User Acknowledgment

I acknowledge that I have received and read the Information Resources Acceptable Use Policy. I understand and agree that my use of University Information Resources is conditioned upon my agreement to comply with the 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:_____

Information Security and Privacy Agreement

UT Health RGV Facilities and other UTRGV subsidiaries (collectively, "UTRGV" or "UTRGV organization") are committed to maintaining high standards of confidentiality. The responsibility to preserve the confidentiality of information in any form (electronic, verbal, or written) rests with each User granted access to UTRGV information systems who may have access to Confidential Information, including Protected Health Information (PHI), Electronic Protected Health Information (ePHI), employee information, physician information, vendor information, medical, financial, or other business-related or company confidential information. Any information created, stored or processed on UTRGV systems, or systems maintained on UTRGV' behalf by a vendor or other individual or entity, is the property of UTRGV, as is any information created by or on behalf of UTRGV, whether written, oral or electronic. UTRGV reserves the right to monitor and/or inspect all systems that store or transmit UTRGV data, the data stored therein, as well as all documents created by or on behalf of UTRGV.

Definitions:

Agreement means this *UTRGV Information Security and Privacy Agreement*.

Confidential Information means confidential information that is created, maintained, transmitted or received by UTRGV and includes, but is not limited to, Protected Health Information ("PHI"), Electronic Protected Health Information ("ePHI"), other patient information, Workforce member information, employee, physician, medical, financial and other business-related or company private information in any form (e.g., electronic, verbal, imaged or written).

Protected Health Information ("PHI") means individually identifiable health information that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. PHI can be oral, written, electronic, or recorded in any other form.

Electronic Protected Health Information ("ePHI") means Protected Health Information in electronic form.

User means a person or entity with authorized access to any UTRGV network and/or other information systems, including computer systems.

Workforce means employees, volunteers, trainees, and persons whose conduct, in the performance of work for UTRGV, are under the direct control of UTRGV, whether or not they are paid by UTRGV. Workforce also include management and employed medical staff.

I HAVE READ AND UNDERSTAND THIS ENTIRE AGREEMENT, AND I AGREE TO THE FOLLOWING:

(Note: Please initial each line in the space provided after reading it.)	***Initials:***
1. I understand it is my personal responsibility to read, understand and comply with all applicable UTRGV company policies and procedures, including Security policies. I understand that these policies provide important information about the acceptable use of information systems, protection from malicious software, Mobile device usage, and data encryption, and other important information. If I am provided access to PHI or ePHI, I also agree to comply with the Privacy policies.	
2. I have been provided access to the Security (and Privacy policies as applicable).	
3. I agree not to disclose any PHI, ePHI or any other Confidential Information obtained by accessing the UTRGV network and/or other information systems, including computer systems, or otherwise to any unauthorized party. I agree not to access or use any PHI, ePHI or any other Confidential Information unless I am authorized to do so. I agree that all patient- related information shall be held to the highest level of confidentiality.	
4. I agree to access the UTRGV network and/or other information systems, including computer systems, only for purposes related to the scope of the access granted to me.	
5. I understand that UTRGV regularly audits access to information systems and the data contained in these systems. I agree to cooperate with UTRGV regarding these audits or other inspections of data and equipment, including UTRGV inquiries that arise as a result of such audits.	
6. I agree that I will not share or disclose User IDs, passwords or other methods that allow access to UTRGV network and/or other information systems, including computer systems, to anyone, at any time, nor will I share my account(s). I also agree to store all UTRGV company- related data onto the system servers rather than on hard drives of individual workstations, personal computers or other devices.	
7. I agree to contact my supervisor (or for non-employees, the applicable UTRGV Department Director or Business Contact) and IS Security Officer immediately if I have knowledge that any password is inappropriately revealed or any inappropriate data access or access to Confidential Information has occurred.	
8. I understand that Confidential Information includes, but is not limited to PHI, ePHI, other patient information, employee, physician, medical, financial and all other business-related or company private information (electronic, verbal or written).	
9. I agree that I will not install or use software that is not licensed by UTRGV (or that is otherwise unlawful to use) on any UTRGV information systems, equipment, devices or networks. I understand that unauthorized software may pose security risks and will be removed by UTRGV.	
10. I agree to report any and all activity that is contrary to this Agreement or the UTRGV Security or Privacy policies to my supervisor, Department Director, IS Security Officer or Privacy Officer.	

11. I understand that for employees this form will be part of the employee file at UTRGV and that failure to comply with this Agreement and the UTRGV Security and Privacy policies may result in formal disciplinary action, up to and including termination. I understand that for non-employees, failure to comply with this Agreement and the UTRGV Security and Privacy policies may result in revocation of access and the termination of any agreements or relationships with UTRGV.	
12. I understand that all information and/or data transmitted by or through or stored on any UTRGV device, or system maintained on any UTRGV company's behalf by a vendor or other individual or entity, will be accessible by UTRGV and considered the property of UTRGV, subject to applicable law. I understand this includes, without limitation, any personal, non- work related information. I do not have any expectation of privacy with regard to information on any UTRGV network and/or other information systems, including computer systems, and understand that UTRGV has no obligation to maintain the privacy and security of the information. I understand that UTRGV reserves the right to monitor and/or inspect all systems that store or transmit UTRGV data, the data stored therein, as well as all documents created by or on behalf of UTRGV.	
13. I agree to comply with UTRGV requirements to encrypt electronic Confidential Information in accordance with UTRGV security policies, including the requirement that encryption software be installed on all UTRGV-owned laptop computers and that emails transmitted over an electronic network outside of UTRGV be encrypted, as described in the UTRGV Security policy *Data Encryption and Decryption.*	
14. I agree that all devices used by me that are connected to a UTRGV network and/or other information systems, including computer systems, whether owned by me or not, will be continually running approved and updated anti-virus software.	
15. I will follow the requirements for Users described in all UTRGV Security policies, including but not limited to the UTRGV Security policy *Acceptable Use Policy.*	
16. I agree to limit access to only patient data specifically relating to assigned patient care. This includes all patient information related to myself, family members, providing direct care to including but not limited to the UTRGV security policy	
17. *I understand that UTRGV has zero tolerance and violation of the UTRGV Information Security and Privacy Agreement will result in disciplinary action up to termination.*	

The UTRGV Information Security and Privacy Policies are available through my supervisor, manager, UTRGV business contact or the UTRGV Information Security Office.

By signing this Agreement, I understand and agree to abide by the conditions imposed above.

_____ _____

Signature Print Name

_____

Date

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: _____