New Student Orientation Security Acknowledgement

The University of Texas Health Science Center at Houston's (UTHSC-H) information resources are owned by the university and are provided to accomplish the university's mission. Users must use university information resources appropriately to ensure availability and preserve information integrity and confidentiality. A user is anyone who is granted access to a university information resource, including, but not limited to faculty, students, residents, staff, alumni, retirees, continuing and distance education students, researchers, principal investigators, visiting faculty, business partners, contractors, vendors, consultants. Any electronic equipment, devices or media that a user connects to the university network or uses to process or store university information, including equipment, devices or media owned by the user or funded by another source, are considered university information resources for the purpose of compliance with laws, regulations and policies.

Use of university information resources is subject to UTHealth and University of Texas System (UT System) policies and state and federal laws, which include, but are not limited to:

- UTHealth Information Technology policies and procedures posted in the IT Policy & Document Repository (https://inside.uth.edu/it/cio/policies/index.htm);
- UTHealth Handbook of Operating Procedures (HOOP) 175, Roles and Responsibilities for University Information Resources and University Data (https://www.uth.edu/hoop/policy.htm?id=1448198);
- HOOP 180, Acceptable Use of University Information Resources (https://www.uth.edu/hoop/policy.htm?id=1448208);
- UT System policy 165, UT System Information Resources Use and Security Policy (https://www.utsystem.edu/board-of-regents/policy-library/policies/uts165-information-resources-use-and-security-policy).

Failure to comply may result in disciplinary action including termination of employment, professional/business relationship, or dismissal from school. Civil and/or criminal sanctions may apply.

I acknowledge I understand my role in protecting information resources. I will uphold/comply with applicable laws and the policies noted above, including the following:

1. University information resources must be secured from unauthorized, accidental or intentional access, modification or destruction.
2. University owned or managed information resources must be used only for university business.
3. All assigned passwords to information resources including, but not limited to, network systems, computer accounts, encryption software, voice mail and long distance telephone codes must not be shared with anyone. Disclosing a password may result in immediate termination of employment, professional or business relationship, or dismissal from school.
4. Users should have no expectation of privacy regarding e-mail use, Internet use or other activities performed on, or information processed by or residing on, university information resources. All e-mail and Internet use can be monitored and stored along with the source and destination. Additionally, all incoming and outgoing e-mail is archived and is subject to the Texas Public Information Act.
5. Software, including electronic media or files, may not be downloaded, copied or otherwise used in violation of the licensing agreement and/or copyright.
6. All information resources are subject to random, unannounced audits to ensure compliance with all university and UT System policies and state and federal laws.
7. It is the responsibility of all users to report any suspected or confirmed violations to appropriate management, to the Chief Information Security Officer (ciso@uth.tmc.edu), or via the confidential compliance hotline (888-472-9868).
8. Users must complete all required initial and recurring information resource training.
9. All sensitive and confidential information, including but not limited to information covered by FERPA and HIPAA (such as SSNs, PHI), must be stored on appropriate network drives; do not save it to your local PC. If university business requires that it be saved on a portable device (e.g. external hard drive, USB device, DVD, CD, etc.), it must be encrypted, the device must be password protected, and it may only be saved temporarily.

McGovern Medical School --- Student Computing Policies

- No Student shall install or download any software on any UTHealth computer(s) without explicit permission.
- No Student may reconfigure or otherwise adjust any settings on any UTHealth computer(s) software or hardware without explicit permission.
- No student may make copies of software which resides on McGovern Medical School computers, with the exception of that found in the shareware directories of the McGovern Medical School WWW server.
- Passwords, or other digital identification, may NOT be shared with ANYONE under any circumstances. You are fully responsible for protecting all confidential information entrusted to you.
- Your UTHealth password should not be used for ANY other website or service (ex. Facebook, LinkedIn, Twitter, etc.)
- No one may attempt to access any system without proper authorization from the appropriate system administrator.

- Patient care information in any form is confidential information. This information may be accessed only by persons who need the information to perform their job functions. Using another person's password to access or enter information into a patient's clinical record constitutes falsification of the medical record.
- Students are responsible for logging off the computer after each use.
- Students must complete the four training modules mandated by the Health Insurance Portability and Accountability Act (HIPAA) of 1996 **immediately**. Please contact Student Affairs for information.
- In order to maintain compatibility with exam software please do not upgrade the operating system to a new version until that operating system version has been approved by MSIT or Educational Programs. Upgrading to an unsupported operating system could prevent you from taking exams using your laptop.

Privacy, Confidentiality, and Information Security Agreement for Patient, Confidential, Restricted and Proprietary Information

All UTHealth workforce members (including faculty, students, employees, trainees, volunteers, guests and other persons who perform work for UTHealth) are personally responsible for ensuring the privacy and security of all patient, confidential, restricted, and proprietary information to which they are given access, including research data and student information (referred to throughout this document as protected information).

I understand and acknowledge the following:

Policies and Regulations

I will comply with UTHealth policies governing protected information.

I will report all concerns about inappropriate access, use or disclosure of protected information, and suspected policy violations to the UTHealth Privacy Hotline (713-500-3391) or the UTHealth Compliance Hotline (1-888-472-9868 or www.tnwinc.com/webreport or by sending an email to compliance@uth.tmc.edu) and to my immediate supervisor.

I will report all suspected security events and security policy violations to the Computer Security Incident Response Team (its@uth.tmc.edu) or the Help Desk (713-486-4848) and to my immediate supervisor.

Confidentiality of Information

I will access, use and disclose protected information only as allowed by my job duties and will limit that access to the minimum necessary to perform my authorized duties. I understand that my access will be monitored to assure appropriate use.

I will keep protected information taken off-site only on UTHealth-approved and encrypted devices.

If I must carry printed protected information on my person to conduct my authorized duties, I will keep it to a minimum and I will keep it in my physical possession during transit, never leaving it unattended or in any mode of transport (even if the mode of transport is locked).

I will only take protected information off-site if accessing it remotely is not a viable option.

Computer, Systems, and Applications Access Privileges

I will only access protected data for job-related duties.

I will protect access to patient and other job-related accounts, privileges and associated passwords.

- I will commit my password to memory or store it in a secure place;
- I will not share my password;
- I will not log on for others or allow others to log on for me;
- I will not use my password to provide access or look up information for others without proper authorization.
- I will not use my UTHealth password on any other website or service

I am accountable for all accesses made under my login and password, and any activities associated with the use of my access privileges. I will only use my own credentials as provided to me for my job duties in accessing protected data and/or systems.

Computer Security

- I will store protected information only on UTHealth-approved and encrypted systems.
- I will not change my UTHealth computer configuration unless specifically approved to do so.
- I will not disable or alter the anti-virus and/or firewall software or encryption software on my UTHealth computer.
- I will ensure that my personal laptop requires a password to log in and to unlock after 15 minutes of inactivity
- I will log out or lock computer sessions prior to leaving a computer.
- I will not store protected data on non-University owned devices or media.
- **I will store my BitLocker encryption key in a secure place** (ex. Microsoft, Google Drive, Dropbox, etc.) and that I will be able to retrieve it (if/when needed) in order to gain access to the data saved on my laptop.
- I understand that MSIT does not have a copy of my BitLocker encryption key.
- **I understand that without my BitLocker encryption key, all data on my laptop is inaccessible and MSIT will not be able to help me retrieve my data.**

Failure to comply with this agreement may result in disciplinary action up to and including termination of my status as a workforce member or expulsion as a student (as described above) at UTHealth. Additionally, there may be criminal and/or civil penalties for inappropriate uses or disclosures of certain protected information.

During the computer orientation, MSIT will verify that all student laptops meet the full disk encryption requirements. Once encryption is verified, MSIT will place orange stickers on the laptops indicating that the laptops are encrypted and that they have been verified by MSIT. The sticker is tamper-evident and should not be removed from the laptops without MSIT approval. Removing or disabling encryption from your laptop while enrolled as a student at the McGovern Medical School at Houston is strictly prohibited. Failure to adhere to this policy will result in disciplinary action. If I purchase a new computer while enrolled as a medical student at the McGovern Medical School, the computer will need to meet the latest incoming class computer requirements.

UTHealth is not responsible for any hardware and/or software issues or data loss that may occur as a result of enabling encryption on your laptop. Please keep the encryption key stored in a safe location as it may be required to unlock your hard drive in order to boot the operating system or recover data. **It is impossible to recover data from an encrypted hard drive without the encryption key.**

By signing this form, you acknowledge that you have read it completely and fully understand the policies described above.

LAST NAME _____ SIGNATURE _____

FIRST NAME _____ DATE _____