UTHealth™ | Medical School
The University of Texas
Health Science Center at Houston

Information Services: Security Acknowledgement Form

Information resources at UT Health (also known as The University of Texas Health Science Center at Houston) are owned by the University and are provided to employees and other users to accomplish the University's mission. Users are expected to use these resources appropriately, to ensure their ongoing availability and preserve information integrity and confidentiality.

A "user" is defined as anyone who is granted access to a university information resource. This includes, but is not limited to: faculty, students, residents, staff, alumni, retirees, continuing and distance education students, researchers, principal investigators, visiting faculty, business partners, contractors, vendors and consultants.

An "information resource" is defined as any electronic equipment, devices or media that a user connects to the University network, or uses to process or store University information. This includes, but is not limited to: computers, servers, monitors, fax equipment, scanners, printers, portable tablets and other peripherals, as well as software, applications (aka "apps") and media used on them.

Note that electronic 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 UT Health and University of Texas System (UT System) policies and state and federal laws, which include, but are not limited to:

- UTHSC-H Information Technology policies and procedures posted in the IT Policy & Document Repository;
- UTHSC-H Handbook of Operating Procedures (HOOP) 175, Responsibility for the Use of Information Resources;
- HOOP 180, Email and Internet Usage;
- UT System Policy 165, UT System Information Resources Use and Security Policy

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

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

Information Security Policies

1. Safeguard all University-owned information resources against unauthorized, accidental or intentional access, modification or destruction.
2. Do not share assigned userids and passwords to information resources with anyone. This includes, but is not limited to, userids and/or passwords for network systems; computer accounts; encryption software; voice mail; and long distance telephone codes.
3. Do not access patient health information (PHI) without authorization. It is illegal to use another person's password to access or edit a patient's clinical record.
4. Store any confidential and sensitive information on appropriate network drives. ***Do not save such data to your local computer hard drive.***

5. Do not replace, tamper with or remove anti-virus or firewall software without explicit approval from MSIT.

Email and Internet Usage Policies

1. You should have no expectation of privacy regarding email use, Internet use or other activities when using University information resources.
2. Be aware that email and Internet usage information is recorded and subject to monitoring. Incoming and outgoing email is archived by the University, and subject to the Texas Public Information Act.
3. Always encrypt emails dealing with confidential or sensitive information, including: patient health information (PHI); information protected by HIPAA and/or FERPA; and human resources data.
4. Place digital signatures on outgoing email whenever applicable and possible to do so.
5. If you need digital signature or encryption capability, apply here for a digital ID, or contact your LAN Manager.

Hardware and Software Usage Policies

1. University-owned or managed information resources must be used only for University business.
2. Other than personally owned handheld telephones, no personally owned computing devices including laptops, desktops, tablets, or peripherals, may be stored or used in any UT Physicians clinic.
3. All computers handling University Data must be encrypted, except where exempted by IT Security. Contact your LAN Manager for details.
4. Only MSIT personnel should install, reconfigure or otherwise adjust any computer system's hardware or software, unless other arrangements are made with your LAN Manager.
5. As specified in the Laptop Security Policy, all laptops must have full disk encryption (FDE).
6. As specified in the Portable Storage Device Policy, data stored on a portable device (external hard drives, USB drives, read-writable DVDs or CDs, etc.) must be password protected.
7. Use encrypted portable devices only for transport purposes, not for long term storage.
8. Do not download, copy, or use software in violation of licensing agreements and/or copyrights. This includes, but is not limited to, software, electronic media, licenses, license keys or codes or installation files.
9. Do not store personal data such as music, pictures, movies, etc. locally or on the network.
10. Unless directed otherwise, do not shut down your computer(s) at the end of your work day. Before leaving, save and close documents. Software updates, when applied, may require your computer to automatically reboot.
11. Do not transfer computers or peripherals to your Department from Surplus without prior MSIT approval.
12. Do not move computers or peripherals without consulting your LAN Manager.
13. Consult with your LAN Manager when seeking to purchase or lease new computers, computer accessories, peripherals or software. The University leases most computers.
14. Computers, peripherals and/or software should be purchased or leased using the online MSIT Lease and Purchase Application.
15. If University owned equipment based at an employee's home requires repair and cannot be fixed remotely, such equipment must be brought in so MSIT can repair it.
16. Employees using University-owned equipment at home must make sure that all data is backed up to secured drives or the University's network, and that the computer's anti-virus software and operating system security patches are kept up to date.
17. Although MSIT assists with minor printer problems, major repair work will be handled by a printer repair vendor. Vendors may require payment before repairs are made unless the printer is under warranty.

Policies for Portable Devices

The UTHSCH HIPAA policy states the following:

> ***PHI (protected health information) should be stored on secured servers in the Secure Zone (formerly called Zone 100).*** The Secure Zone is a protected area on the Medical School's network, also called the NAS. The NAS is backed up several times daily, to protect data from being lost through accident or misadventure.

1. All Medical School employees should have a drive mapped to the NAS on their PCs, and they should save their data – including PHI data – exclusively to that drive, never to local PCs or laptops or unsecured flash drives. (If you do not have access to a mapped NAS drive, contact your LAN Manager.)
2. Portable computing devices – including laptops, tablets, USB (flash) drives and PDAs – should be kept secure by remaining in the department or by password protection.
3. All portable devices should be encrypted.
4. If transient PHI must be stored on portable computing devices like laptops, PDAs and flash drives, the data must be encrypted, and the device password protected.
5. When using laptops, tablets or PDAs, save all data to network drives or encrypted USB drives, never to the portable device.
6. ***Only encrypted USB flash drives may be purchased.*** For more information, visit the Medical School's Approved Portable Devices page or contact your LAN Manager. Remember that any data not backed up on a regular basis may be lost if your computer crashes.

Remember that any email that contains identifiable patient information must be digitally encrypted before it is sent. Digital IDs are necessary to encrypt emails, and can be obtained by contacting your LAN Manager.

Other Policies

1. Complete all initial and recurring information resource training as required.
2. Do not disable your screen saver, or increase the 15 minute activation time.
3. Be aware that information resources are subject to random, unannounced inspection audits to ensure compliance with all university and UT System policies and state and federal laws.
4. Specialized computers, including those used in research, may be granted exceptions from some of these policies. Contact your LAN Manager for more information.
5. Report suspected or confirmed violations of information resources or data to your supervisor or LAN Manager. If necessary, you can also contact MSIT management or the confidential Compliance Hotline (1-888-472-9868).
6. For support with information resources, please fill out a help desk ticket at https://msitapps.uth.tmc.edu/mshelpdesk/.

By signing this form, you acknowledge that you have read it completely and fully understand the policies described above. Please print on the lines below:

LASTNAME: ____

FIRST NAME: ____

DEPARTMENT: ____

ROOM #: ____

SIGNATURE: ______________________________ DATE: __________