HEALTH SCIENCE CENTER
TEXAS A&M UNIVERSITY

Data Use and Confidentiality Agreement

Access to Technology and Information Resources

Access to Texas A&M Health Science Center data and information, and access to IT accounts, systems, and applications, is based on your need for access and your assent to use that access appropriately. These services are integral to the operation of the university, and security and privacy laws and other institutional policies protect much of the information.

Therefore, before you can be granted access, you must read and agree to follow these acceptable usage standards, and must accept responsibility to preserve the security and confidentiality of information that you access, in any form, including oral, print, or electronic formats.

Although these general provisions apply to all Health Science Center information and IT accounts, systems, and applications, please be aware that managers of certain services or information types may require you to complete additional agreements and/or training.

Usage responsibilities:

The following points detail your responsibilities as you access, use, or handle information or information technology (IT) at Texas A&M Health Science Center.

Secure Usage

You agree to:

- Never share your account password(s) or passphrase(s) with anyone.
- Select strong password(s) and passphrase(s).
- Be mindful that different computer systems and applications provide different levels of protection for information, and seek advice on supplemental security measures, if necessary. For example, a mobile laptop provides inherently less protection than a desktop computer in a locked office. Therefore, the level of protection provided to information accessed or stored using a laptop is to be supplemented by using additional safeguards such as encryption technology, enhancing physical security, restricting file permissions, etc.
- Respect the university's information and system security procedures (i.e., never attempt to circumvent or "go around" security processes).
- Maintain information in a secure manner to prevent access, viewing, or printing by unauthorized individuals.
- Secure unattended devices (e.g., log off, lock, or otherwise make inaccessible), even if you will only be away from the computer or device for a moment.
- Store Restricted and Critical data securely (e.g., on secure servers, in locked file cabinets, etc.).
- Securely dispose of Restricted and Critical information (e.g., by shredding, disk wiping, physical destruction, etc.).
- Never copy and/or store Restricted or Critical data outside of institutional systems (e.g., on desktop workstations, laptops, USB drives, personally owned computers, etc.) without proper approval from the senior executive officer of the department and only in cases where it is absolutely necessary for the operation of the department.
- Take appropriate steps to secure information (e.g., password protection, encryption, etc.) on mobile storage devices (e.g., laptops, USB drives, cell phones, etc.).
- Ensure, in the rare cases where Critical data has been approved for use and storage outside of institutional systems, that the data are appropriately encrypted, especially on mobile storage devices (e.g., laptops, cell phones, USB drives, CD-ROMs).
- Ensure, in the rare cases where it is necessary to email Critical or Confidential data, that the data are sent to the correct recipient and only via encrypted email methods.

- All PHI stored on electronic devices will be de-identified where applicable.

Legal Usage

You agree to:

Use information and resources for legal purposes only.

- Respect and comply with all copyrights and license agreements.
- Never use your access to information or devices to harass, libel, or defame others.
- Never damage equipment, software, or data belonging to others.
- Never make unauthorized use of computer accounts, access codes, or devices.
- Never monitor or disrupt the communications of others, except in the legitimate scope of your assigned duties.
- Abide by applicable laws and policies with respect to access to, use, disclosure, and/or disposal of information. Applicable law and policies include but are not limited to:
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Family Educational Rights and Privacy Act (FERPA)
    - TAMHSC rules and policies (http://www.tamhsc.edu/facultystaff/rules/)

Ethical Usage

You agree to:

- Access institutional information only in the conduct of business and in ways consistent with furthering the mission of education, research, and public service.
- Use only the information needed to perform assigned or authorized duties.
- Never access any institutional information to satisfy your personal curiosity.
- Use information and IT in ways that foster the high ethical standards of the university.
- Never use information or IT to engage in academic, personal, or research misconduct.
- Never access or use institutional information (including public directory information) for your own personal gain or profit, or the personal gain or profit of others, without appropriate authorization.
- Respect the confidentiality and privacy of individuals whose records you may access.
- Preserve and protect the confidentiality of all internal, restricted, or Critical information as matter of ongoing responsibility.
- Never disclose internal, Restricted, or Critical data (as defined by policy; see above) or distribute such data to a third party in any medium (including oral, paper, or electronic) without proper approval, and in the case of Restricted or Critical data, without a contract processed through or waived by the Health Science Center Purchasing Department.

To be entrusted with acces to Texas A&M Health Science Center data and information, and acces to IT accounts systems, and applications, all users must accept these responsibilities and standard or acceptable use. By accepting these terms, you agree to follow these rules in all of your interactions.

I have read, understand, and agree to abide by the practices outlined in this agreement.

Name (Print)_____ Account Name_____

Signature _____ Date _____