Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.22	**Data Protection**	Responsibility:	Chief Information Security Officer

DATA PROTECTION

Policy

The UT Health San Antonio Policies, Standards and Procedures must describe and require steps to protect University data using appropriate administrative, physical and technical controls in accordance with the Information Security Program, Data Classification policy, UTS 165 and its associated Standards, and any federal or state law and regulation that may apply to the data's classification.

Password and Encryption Protection

All high risk desktop computers, laptop computers and mobile devices, including but not limited to, smartphones and tablet computers, that are owned, leased, or controlled by UT Health San Antonio must be encrypted using methods approved by the Chief Information Security Officer. Access to these devices must be password protected in compliance with UT Health San Antonio policy.

USB and similar removable storage devices owned, leased, or controlled by UT Health San Antonio must be encrypted before confidential data is stored on the device.

All personally owned computing devices, mobile devices, USB storage devices or similar devices must be password protected and encrypted using methods approved by the Chief Information Security Officer if they contain any of the following types of data:

- information classified as "Confidential";
- federal, state, university or privately sponsored research that requires confidentiality or is deemed sensitive by the funding entity; or
- any other information that has been deemed by UT Health San Antonio as essential to its operations to the extent that its integrity and security should be maintained at all times.

Assured Access to Encrypted Data

For all computing devices owned, leased or controlled by the UT Health San Antonio, Standards and/or Procedures shall be defined and documented to ensure accessibility of encrypted data in the event that an encryption key becomes corrupted or unavailable.

For personally owned devices protected by provisions described in this and other UT Health San Antonio policy, the device owner is responsible for ensuring that encrypted data is backed up to UT Health San Antonio owned or sanctioned storage.

Data in Transit

UT Health San Antonio shall adopt and document Policies, Standards, and/or Procedures and implement appropriate administrative, physical and technical safeguards necessary to adequately protect the security of data during transport and electronic transmissions. Each of the following controls shall be addressed:

a. Prior to disposal or repurposing storage media, original records subject to retention requirements must be copied to an alternative storage device. Original records must be accessible and retrievable for mandated retention periods, as documented in the institution's "Record Retention Schedule". The alternative data device and all other removable media must be protected commensurate with the data stored on them.

b. Information Resource Owners must remove all data contained on storage media prior to transferring it to the UT Health San Antonio warehouse for disposal or repurposing. Prior to disposal of data storage media the Information Resource Owner must certify that no data remains on the media or device. For common rotating magnetic media (hard drives), the departmental Technical Support Representative (TSR) is authorized to use software designated by the Chief Information Security Officer that will destroy all data on the drive.

c. Prior to repurposing a storage device or media that previously contained "Confidential" or "Confidential/High Risk" information, the data on the media must be completely destroyed using a process approved by the Chief Information Security Officer.

Storage and Transport of Electronic Media

Information Resource Owners, in coordination with the Chief Information Security Officer, shall adopt and document physical and technical controls for securing storage devices and removable media that contain Confidential data. These Standards and Procedures should include, but are not limited to, movement of the media, access to the media, its storage, and its transfer to other parties.

Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.22	**Data Protection**	Responsibility:	Chief Information Security Officer

Accountability

Violations of this policy are subject to disciplinary action as described in Section 2.1.2, "*Handbook of Operating Procedures*".

References

- U.T. System Policy 165 Standard 11
- HIPAA Security Rule 164.312(a)(2)(iv)
- HIPAA Security Rule 164.312(e)(2)(ii)