Chapter 11	Patient Privacy Policies	Effective:	April 2010
Section 11.1	General and Oversight Policies	Revised:	March 2013
Policy 11.1.14	**Securing Protected Health Information and Mobile Devices**	Responsibility:	Chief Compliance Officer for Regulatory Affairs & Compliance

SECURING PROTECTED HEALTH INFORMATION AND MOBILE DEVICES

Policy

The Health Science Center has developed several institutional policies to ensure the protection and security over sensitive and confidential information. These policies also cover patient health information. The policies are located in Chapter 5 of the *Handbook of Operating Procedures* (HOP).

Below are some policies that must be implemented when handling patient health information.

- E-mails sent outside of the Health Science Center (other than uthscsa.edu address) must be encrypted. This is done by placing two plus symbols (++) at the beginning of the "subject" line and before the subject of the message. Also, if an e-mail is subsequently forwarded or replied to, the ++ must be placed in the "subject" line of the message before the "FW" or "RE". See Section 11.1.12, "E-mailing Protected Health Information" of the HOP.

- Patient health information, when sent digitally, must always be transmitted in an encrypted manner. This includes wireless transmissions and faxes.

- Institutional laptops or tablets must be encrypted with an institutionally-approved encryption software or protected by some other compensating control approved by the Chief Information Security Officer. Patient information shall not be downloaded onto personally owned mobile devices, including mobile storage devices (e.g., CD, DVD, flash drive, external hard drive). See Section 5.8.12, "Portable Computing Policy" and Section 5.8.22 "Storage Media Control" of the HOP.

- Patient health information should never be stored on social networking Web sites or transmitted through peer-to-peer applications. See Section 5.8.11, "Peer-to-Peer Access Policy" of the HOP.

- Individually assigned passwords that allow access to electronic health records shall not be shared with others. See Section 5.8.4 "Access Control and Password Management" of the HOP.