11.1.14 Securing Protected Health Information and Mobile Devices

Chapter 11 - Patient Privacy	Original Effective Date: April 2010
Section: 11.1 General and Oversight Policies	Date Last Reviewed: January 2023
Responsible Entity: Chief Compliance and Privacy Officer	Date Last Revised: January 2023

I. Purpose

To ensure the protection and security of sensitive and confidential protected health information on mobile devices.

II. Scope

This policy applies to all faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other individual (collectively, Workforce Member, including employees and non-employees) who has direct or indirect access to patient protected health information (PHI) created, held or maintained by any UT Health San Antonio controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

A. Emails sent outside of UT Health San Antonio (other than uthscsa.edu address) must be encrypted. This is done by placing two plus symbols (++) in the subject line. This tells the university's email system to transmit the message securely.

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

C. 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.

D. Patient health information must not be stored on personally owned mobile devices, including mobile storage devices (e.g., CD, DVD, flash drive, external hard drive. See HOP policy 5.8.12 Mobile Device and Personally Owned Computing Policy.

E. Individually assigned passwords that allow access to electronic health records shall not be shared with others. See IHOP policy 5.8.4 Access Management.

IV. Definitions

Terms used in this document, have the meaning set forth in the Patient Privacy Policies Glossary *unless a different meaning is required by context.*

V. Related References

For questions regarding this policy contact the privacy program director at 210-567-2014 or compliance@uthscsa.edu.

Institutional Handbook of Operating Policies (IHOP)
Chapter 5 - Information Technology, Section 5.8 Information Security

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
04/2010	Policy Origination		
03/2013	Policy Revision		
01/2023	Policy Review	ICPO	01/18/23