Mobile Device and Remote Access Policy

Official Title: Mobile Device and Remote Access Policy
Responsible Office: Information Security
Originally Issued: October 2012
Revised: N/A

INACTIVE

Policy Statement

Georgia Health Sciences Medical Center (GHSMC), Georgia Health Sciences Medical Associates (GHSMA), and Georgia Health Sciences University (GHSU), collectively "GHS" discourages the storage of electronic Protected Health Information (ePHI) as well as other forms of confidential information on mobile devices. The Institution recognizes that incidental storage may occur through normal business activities; therefore, devices used for official business must adhere to the controls outlined in this policy.

Reason For Policy

To define the policy and guidelines for the authorization, connectivity, use, storage, and transmission of GHS data and information systems when using mobile devices and/or use of computers outside of the enterprise's protected network.

Entities Affected By This Policy

This policy applies to all GHS workforce members and is specific to any mobile device or electronic medium designed for storage of data and/or the use of other equipment (e.g. home computers for remote access) used to conduct GHS business activities outside of the organization's technical control and management, regardless of ownership.

Who Should Read This Policy

All employees of a GHS entity should read and be aware of this policy.

Contacts

Contact	Phone	e-mail/URL
Walter Ray, CISO	(706) 721-1577	security@georgiahealth.edu

Related Documents

None

Definitions

Confidential Information: Any data regulated by federal, state, and/or local statutes or policy. This includes, but is not exclusive to protected health information, personally identifiable information about students or research subjects, information that could be used for identity theft, or data deemed business sensitive such that unauthorized disclosure could have negative impact on GHS operational, financial, or reputational business relations.

INACTIVE

Encryption: Process for transforming information to make it unreadable to anyone except those possessing appropriate credentials to authorize access. Encryption solutions can be obtained and implemented with the assistance of IT Services.

Mobile Device: Any computing device that is easily transported. For the purpose of this policy a mobile device includes handheld computers, smartphones, laptops, tablet computers, USB flash drives, and portable hard drives.

Remote Access: Using any device, regardless of ownership, to access GHS information or information systems from outside the enterprise network. Examples would include: virtual private network (VPN), email access offsite, Citrix web access offsite, etc.

Remote Wipe: Process in which data can be remotely deleted from a mobile device.

Smart Phone: Any mobile phone that, in addition to basic voice communications, offers advanced computing ability, data storage, email, and/or Internet connectivity.

Rooting or Jailbreaking: Installing software or exploiting an OS flaw that bypasses the security lockouts enforced by the manufacturer on a mobile device.

Overview

Provisions

1. All mobile computers and devices, regardless of ownership, used to conduct the business of the enterprise must meet the security standards outlined in this policy as well as those referenced in Related Policies section below. The institution expects all users to utilize appropriate enterprise designated systems for the storage of patient information (i.e., Synchronicity is the system of record for the electronic medical record).
2. Storage or transmission of ePHI or Confidential Information to Internet based websites, to include but not exclusive to, social networking sites (e.g. Facebook, Twitter, Google Docs) is strictly prohibited unless explicitly approved by GHS CISO and GHS CERM / Legal Offices. Any approvals granted must be supported by legally binding contracts and Business Associate Agreements as applicable.
3. Requests for approval to store or transmit ePHI to mobile and/or remote devices may be submitted through the IS Service Request system.
4. Remote Access to ePHI. Remote access to ePHI is only granted to authorized users based on role within the organization and must connect using a GHS approved / secure standard for data transmission. (Refer to the General Technical Requirements and Device Specific Requirements sections of this policy for more information.)
5. Security Responsibility. All workforce members are responsible for the protection of ePHI and GHS owned data contained on mobile or remote devices in their custody and/or used to connect to the GHS network. Security of data maintained, stored, or transmitted is subject to the provisions of local, State, and Federal statutes and regulations, and the provisions of GHS privacy and security policies.

General Technical Requirements

1. Virus Protection. Any system used to connect to the GHS network or other business entity on behalf of GHS, regardless of location or ownership must have safeguards installed to prevent virus infection or unauthorized access to the GHS network or data.
2. Mobile or remote devices connecting to GHS systems or used for official business must:
   - be password protected,
   - use GHS issued and installed data encryption software to prevent unauthorized disclosure,
   - as applicable, have personal firewalls installed and active,
   - never be left unattended and remain in positive control of the custodian at all times, and
   - be permanently destroyed when no longer required, the system has reached end of life, or ownership is transferred.
3. Security Software. No action should be taken to disable security software or configurations designed to protect the device from compromise. This includes removal of anti-virus software or disabling firewalls on a laptop and rooting or jail-breaking a phone or tablet.

Device Specific Requirements

1. **Laptops.** Laptops must employ a GHS approved software encryption package. All new GHS purchased laptops must be configured with GHS administered remote management software (e.g. Computrace) to allow tracking and recovery of lost or stolen devices.
2. **Smart Phones and Tablets**. All smart phones, tablets, and PDA's used to connect to GHS information systems (including email) must adhere to standards defined under paragraph 7 of this policy with a minimum password length of 4 characters and configured to a timeout of no greater than 10 minutes of inactivity. All GHS smart phones, tablets, PDAs, regardless of ownership, connected to the GHS enterprise information systems and email resources must be configured through GHS mobile device management services. GHS reserves the right to wipe any smart phone or tablet connecting to GHS systems. This is especially relevant to devices connecting to the GHS email system or

other systems which download data to the device's onboard data storage.

3. **USB (Thumb) Drives and Portable Hard Drives.** All USB and portable hard drives storing GHS owned confidential data must be encrypted using an approved method of encryption to protect data at rest.
4. **Lost or Stolen Computer Equipment** must be reported immediately to Public Safety, GHS Security and/or Information Security Office. Information regarding loss or theft will be shared between entities as required. The GHS workforce member with custodial responsibility for the device preceding the incident of theft will be required to complete a Lost/Stolen equipment report describing the data contents of the device and to assist with recovery, device wipe, and breach investigation as applicable.
5. **End of Life / Surplus.** All mobile devices authorized for connection to GHS information resources must be properly cleansed of all data prior to surplus, trade-in, or redistribution. Contact your GHS Information Security Office for device specific information for cleansing and disposal.
6. **Technical Specifications.** Questions regarding specific technical specifications associated with securing a mobile or remote device can be found by contacting your Information Security Office.
7. **Applicant Validation**. Applicants will be verified against the institution's professional or employee master files in order to validate the applicant's status and privileges.
8. **Enforcement.** Any workforce member found to have violated this policy will be subject to disciplinary action, up to and including termination of employment.
9. **Requests for Exception to Policy**. Requests for exception to this policy should be addressed to the Chief Information Security Officer.

Responsibilities

The responsibilities each party has in connection with this policy, are:

Party	Responsibility
Chief Information Security Officer	Responsible for management and oversight of Mobile Device and Remote Access Policy
All Georgia Health Sciences faculty, staff, and students	Responsible for adhering to the Administrative Policies of the Georgia Health Sciences University and Georgia Health Sciences Health System.

Forms

ISD Service Request System – http://hi.georgiahealth.edu/service_request/

Lost/Stolen Equipment Report – Instructions & Form -http://www.georgiahealth.edu/gchc/gchc/documents/Lost_Stolen_Equipment_Report_Form_Instructions.pdf

This entry was posted in *Administrative*, *Information Technology Support & Services* and tagged *incidental storage*, *Mobile device policy*, *remote access policy*. Bookmark the *permalink*. Both comments and trackbacks are currently closed.

« *Substantive Change Policy*

INACTIVE