UF HEALTH SHANDS CORE POLICY AND PROCEDURE

POLICY NUMBER: CP03.012
CATEGORY: Compliance

TITLE: Mobile Device Management

POLICY: Mobile Devices used to communicate Protected Health Information are limited to individuals involved in the provisioning of direct patient care.

All Mobile Devices used to communicate Protected Health Information or other Restricted Data must be encrypted and utilize approved and encrypted communication channels to transmit or share Protected Health Information. Mobile devices purchased with Hospital funds, including, but not limited to contracts, grants, and gifts, must also be recorded in the unit's information assets inventory.

Hospital Information Security policies applicable to desktop or workstation computers also apply to Mobile Devices. Hospital Confidentiality Policies are also applicable to users of Mobile Devices.

This policy also applies to all students who may access, use or store Protected Health Information in Mobile Devices.

Persons violating this policy may be subject to disciplinary action up to and including termination of their relationship with UF Health and denial of future access to a UF Health information system. In addition, persons improperly accessing, modifying, or disclosing Protected Health Information may be held personally liable. When appropriate, law enforcement, the Department of Health & Human Services (HHS), and/or applicable licensing boards will be notified of incidents.

PURPOSE: To establish Mobile Devices acceptable use standards and safeguards to support clinical care while maintaining the confidentiality, availability and integrity of Protected Health Information.

APPROVED:

Edward Jimenez

Digitally signed by Edward Jimenez
DN: cn=Edward Jimenez, o=UF Health Shands, ou, email=edward.jimenez@shands.ufl.edu, c=US
Date: 2014.11.03 15:06:30 -05'00'

Edward Jimenez
Interim Chief Executive Officer

DEFINITIONS:

A. **Encryption** – the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key (e.g., the translation of data into a secret code).

B. **Health Information** – any information, including genetic information, whether spoken or recorded in any form that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

C. **Individually Identifiable Health Information** – information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

   a. That identifies the individual; or

   b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

D. **Mobile Devices** – Devices intended primarily for the access to or processing of data, which can be easily carried by a single person and provide persistent storage. New products with these characteristics appear frequently. Current examples include, but are not limited to, the following types of products:

1. Laptop, notebook, netbook and similar portable personal computers

2. Smartphones and PDAs (e.g., Android, Blackberry, iPhone, and others).

3. USBs (e.g. flash drives)

E. **Protected Health Information (PHI)** – individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI does not include individually identifiable health information that is in education records covered by the Family Educational Rights and Privacy Act (FERPA), in employment records held by a covered entity in its role as employer, and regarding a person who has been deceased for more than 50 years.

F. **Restricted Information** – Data in any format collected, developed, maintained or managed by or on behalf of UF Health Shands, or within the scope of UF Health Shands' activities that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to, Protected Health Information, medical records, Social Security numbers, credit card numbers, Florida driver licenses, UF student records, and export controlled data.

CORE PROCEDURE:

I. Acceptable Methods for Using or Sharing Protected Health Information (PHI) on Mobile Devices.

A. AMCOM – enterprise communication software that offers HIPAA-compliant texting.

B. HAIKU – software for smartphones (i.e., iPhones) intended to securely connect to the electronic health record.

C. CANTO – like "Haiku for iPads," software intended to securely connect to the electronic health record.

D. Cisco Jabber – an all-in-one communication tool which unifies presence, instant messaging, video, voice messaging, desktop sharing, and conference capabilities securely into one client on a user's desktop; often used with telemedicine.

E. Citrix Receiver – application for smartphones and personal data assistants intended to run the Epic Hyperspace application.

F. VMWare Horizon Client – application that allows users to securely access a virtual desktop.

G. Vidyo – a communication tool that provides video conferencing capability and integrates with mobile devices; often used with telemedicine.

H. E-mail from and to a recipient with a "ufl.edu" e-mail address and when both the sender and receiver have a professional need to know the PHI shared.

I. Epic hand-held software – software for smartphones intended to securely connect to the electronic health record (e.g. Rover application for barcoding medication administration).

NOTE: Other communication means and software specifically excluded from acceptable methods includes, but is not limited to, Twitter, Facebook, Instagram, LinkedIn, Flickr, Shutterfly, or sending PHI using non-approved enterprise software.

II. User Groups Permitted to Use Mobile Devices to Communicate PHI

A. Physicians – directly engaged patient care.

B. Employees – directly engaged in patient care or quality review of patient care. Examples include Nurse Practitioners, Physician Assistants, Nurses, Radiological Technicians, Pharmacists, Risk Managers, and Quality Improvement Specialists.

C. Students – participating in a clinically affiliated educational program (e.g., UF, Santa Fe College) during on-site practicums while in the hospital.

III. Acceptable Uses of Mobile Devices.

A. Facilitating the delivery of immediately needed patient care.

B. To provide mass communication during medical emergencies / disasters.

C. Examples of acceptable uses of Mobile Devices to Communicate PHI:

1. A resident physician photograph's patient's wound and sends image (using HAIKU) to the Attending physician for the immediate delivery of care.

2. A nurse texts stat lab results (using AMCOM) to the ordering physician.

3. A resident takes a photograph of a patient's ECG and sends that image (using AMCOM) to a cardiology fellow for immediate review.

4. A Risk Manager sends an e-mail to an on-call pharmacist (from and to a "ufl.edu" e-mail account) requesting review of a drug currently prescribed to a patient admitted to the hospital.

5. A Quality Director sends an e-mail to a hospital administrator (from and to a "ufl.edu" e-mail account) regarding quality review of adverse incident.

D. Users sharing and receiving PHI must have a professional need to know the information used or shared for treatment purposes.

E. If not already part of the patient's record, communications and/or images used for medical decision making must become part of the patient's health record. See Core Policy 01.035 Records Management.

IV. Unacceptable Uses of Mobile Devices.

A. Examples of unacceptable uses of Mobile Devices to communicate PHI include, but are not limited to, the following:

1. Taking patient photographs out of curiosity.

2. Sharing PHI under the auspices of general medical education.

B. Auto-forwarding e-mail to any external email system outside the ufl.edu domain (e.g., emailing PHI to a G-mail, Hotmail, AOL, or to other similar external email account).

C. Posting PHI or other Restricted Data on social media sites (e.g. Twitter, Facebook).

D. Sharing PHI or other Restricted Data using non-approved software is also unacceptable.

E. Use of Google Glass is prohibited on UF Health Shands-owned property.

V. User Responsibilities

A. Complete Mobile Device Training.

B. Download and Use Approved Software.

1. Contact AHC IT with any questions regarding approved software.

2. Approved software to communicate PHI or other Restricted Data includes:

a. AMCOM,

b. HAIKU,

c. CANTO,

d. Cisco Jabber,

e. Citrix Receiver,

f. Vidyo,

g. VMWare Horizon Client.

h. Epic hand-held software.

i. E-mail to and from a "ufl.edu" account when both the sender and receiver have a professional need to know the information shared.

C. Use Proper Authentication Practices and Passwords.

1. The Mobile Device must be configured to require a strong password of its user and administrator, consistent with or exceeding UF Health Shands password requirements.

2. Portable computing devices where keyboard entry is cumbersome (e.g., Smartphones) may use reduced password complexity if the Mobile Device is configured to allow no more than 10 failed password entry attempts before the device auto-locks.

3. Mobile Devices must be configured with an inactivity timeout of not more than 10 minutes, which requires re-authentication before use.

4. Users are responsible for any activity originating from their Mobile Devices.

D. Encrypt the Mobile Device.

1. All smartphones that access, use or store PHI or other Restricted Data must utilize encryption. The only exceptions to the encryption requirement are for specific uses where no PHI or other Restricted Data will be stored and encryption would interfere with the device's intended use.

2. PHI must be protected by encryption during transmission over any wireless network and any non-UF Health wired network.

E. Security of Mobile Devices

1. Use either a durable physical or electronic label with contact information sufficient to facilitate return (i.e. LoJack for laptops)

2. Use and store the Mobile Device in a manner that deters theft.

3. Users shall immediately report any lost or stolen Mobile Devices to their direct supervisor or chair and to either the AHC IT or to the UF Office of Information Security and Compliance.

4. Use tracking and recovery software whenever possible.

5. Disruptive use of IT resources is not permitted. Occasional personal use of IT resources by employees is permitted when it does not consume a significant amount of those resources, is otherwise in compliance with this policy, and meets with the approval of the supervisor.

F. Ensure Proper Disposal of Devices

1. Disposal of mobile computing and storage devices must be in compliance with the Information Security Electronic Media Control, Disposal and Reuse policy.

2. Contact the AHC IT or place a Computer-Related IT Service Request.

ASSOCIATED POLICIES:

CP01.035 – Records Management and Retention Schedule
CP01.095 – Medical Record Documentation Requirements

Appendix A

Overview of Steps to Take Using Your Mobile Device

1. Use only approved software (e.g. AMCOM, HAIKU, CANTO, etc.) and approved communication methods (e.g. sending text by AMCOM, e-mailing to and from the ufl.edu domain, etc.).

2. Make sure that you're part of a user group (e.g., physician, employee, student) that should be using Mobile Devices to communicate PHI.

3. Communicate PHI for approved purposes, such as the direct immediate provisioning of care.

4. Encrypt your Mobile Device.

5. Ask for help encrypting your device or downloading software.

6. Report any "Oops!" moments should you accidentally communicate PHI inappropriately or if you lose your Mobile Device.

Appendix B

Frequently Asked Questions

What is encryption?

An "invisible" security mechanism that translate data or information in such a way that a device (or computer) with the correct key and unlock or read it. Encryption works by using **ciphers** (also called algorithms) which are specific codes that involve substitutions or transpositions of letters and numbers. Ciphers are also the guides for encryption -- they provide a way in which to craft a message and give a certain range of possible combinations. A **key**, on the other hand, helps a device figure out the one possibility on a given occasion to unencrypt and read the data.

What data must be encrypted?

All Protected Health Information (PHI) and other Restricted Data stored on Mobile Devices, regardless of ownership of the device, must be encrypted.

What is Restricted Data?

Data in any format collected, developed, maintained or managed by or on behalf of the UF Health Shands, or within the scope of UF Health Shands activities that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to medical records, health information, Social Security numbers, credit card numbers, Florida driver licenses, non-directory student records, research protocols and export controlled technical data.

What is considered a mobile device?

Small devices intended primarily for the access to or processing of data, which can be easily carried by a single person and provide persistent storage. New products with these characteristics appear frequently. Current examples include, but are not limited to, the following types of products:

- Laptop, notebook, netbook and similar portable personal computers
- Smartphones (Android, Blackberry, iPhone, and others)

What is considered a mobile storage device?

Media that can be easily carried by a single person and provide persistent storage. New products with these characteristics appear frequently. Current examples include, but are not limited to, the following types of products:

- Magnetic storage devices (diskettes, tapes, USB hard drives)
- Optical storage devices (CDs, DVDs, magneto-optical disks)
- Memory storage devices (SD cards, thumb drives, etc.)
- Portable devices that make nonvolatile storage available for user files (cameras, MP3 and other music players, audio recorders, smart watches, cell phones)

What devices must be encrypted?

All mobile computing and storage devices purchased with UF Health Shands funds, including, but not limited to contracts, grants, and gifts are within scope. All mobile storage devices must be enabled with encryption. The only exceptions to this are for specific uses where no restricted data will be stored and encryption would interfere with the device's intended use.

Who is responsible for encrypting mobile computing and storage devices purchased with UF Health Shands funds?

All UF Health Shands Department Heads, directors and managers, in conjunction with their AHC IT support teams, are responsible for migrating all existing uses of mobile computing and storage devices within their areas of responsibility to devices and services that are compliant with this policy.

Do personally owned mobile computing and storage devices have to be encrypted?

Yes, if the device is used to access or store UF or UF Health Shands Restricted Data.

What devices are required to be inventoried?

Mobile computing devices purchased with UF Health Shands funds must be recorded in the unit's information assets inventory. Mobile storage devices, including USB flash drives and CD or DVD media, do not need to be inventoried.