1. PURPOSE

The purpose of this policy is to define the security requirements needed to protect the confidentiality, availability and integrity of Protected Health Information (PHI) stored on mobile computing devices.

2. POLICY

The use of mobile devices, including personally-owned devices, to access university information has become pervasive. Although this use fosters increased convenience and productivity, mobile devices and the information stored on them and accessed from them are at increased risk of inappropriate exposure due to loss or theft. Therefore, to mitigate this risk, additional safeguards must be applied to mobile devices used to access university information.

Any mobile computing device, including personally-owned devices, accessing IU data is subject to all Indiana University and Indiana University School of Medicine policies. If the capability exists, all mobile computing devices will be configured to:
   a. receive periodic security updates from the operating system vendor
   b. have anti-virus software enabled, active, and up-to-date
   c. have encryption enabled and active
   d. have an application-level firewall installed and active

3. SCOPE

This policy applies to all Indiana University School of Medicine (IUSM) GME resident physicians.

4. DEFINITIONS

4.1 ACGME is the Accreditation Council for Graduate Medical Education.

4.2 A resident is an IUSM resident or fellow, or a non-IUSM resident or fellow electively rotating through IUSM and provides clinical care as part of a GME program.

4.3 Standard - Standards (like procedures) support policy by further describing specific implementation details (i.e. the “how”). A standard can be thought of as an extension of policy that articulates the rules, mechanisms, technical or procedural requirements or specifications to be used in carrying out or complying with a policy. Standards, along with procedures, promote a
consistent approach to following policy. Standards make policies more practically meaningful and effective. Standards are definitional and clarifying in nature specifying the minimums necessary to meet policy objectives. Because standards directly support policies, compliance with standards is non-optional and failure to follow standards may result in sanctions imposed by the appropriate university office.

4.4 Institutional data (or information) - data is considered institutional data if it meets one or more of the following criteria: 1) The data is relevant to planning, managing, operating, or auditing a major administrative function of the university, 2) The data is referenced or required for use by more than one organizational unit, 3) The data is used to derive a data element that meets these criteria. Source: Policy DM-01.

4.5 Critical Data (or information) - Inappropriate handling of this data could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, and/or unauthorized access to this type of information by an individual or many individuals. Source: Classifications of Institutional Data.

4.6 Mobile computing device - includes electronic devices that are capable of accessing, storing, and manipulating information in an untethered manner (usually, but not always, through a wireless connection). This includes laptop and notebook computers, personal digital assistants, Smart Phones, tables and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations.

4.7 HIPAA – is the Health Insurance Portability and Accountability Act of 1996

4.8 PCI-DSS – is the Payment Card Industry (PCI) Data Security Standard (DSS)

4.9 PHI – is protected health information

4.10 UIPO – is the Indiana University Information Policy Office

5. PROCEDURE

A. Safeguard Standards
   a) All mobile devices used by faculty, staff, affiliates, or student-employees to access, store or manipulate institutional data must:
      i. have appropriate safeguards applied to mitigate the risk of information exposure due to loss or theft (see table below). These safeguards may be verified at the university’s discretion and promoted via technical means.
      ii. be reported to it-incident@iu.edu if lost, stolen, or otherwise compromised.
      iii. be wiped before transferring ownership (e.g. sales or trade-ins)
b) Required Safeguards by Device Type

1. Handheld Mobile Device  
   (i.e. Smart Phone, Tablet, etc.)
   
   i. Passcode/Passphrase- Required-minimum 4-character passcode using at least 2 unique characters, and auto lock after a maximum of 15 minutes of inactivity
   
   ii. Intrusion Prevention- Required- lockout or wipe after 10 incorrect attempts, OR Increasing delay after incorrect attempts
   
   iii. Encryption- Recommended in all cases if supported by the device Required for all intended use involving critical information [1]
   
   iv. Remote Wiping- UIPO Incident Response or the Support Center will assist with remote wiping based on the circumstances of reported loss or theft.

2. Laptop or Notebook Computer
   
   i. Passcode/Passphrase- Required-Passphrase meeting IU requirements must be used when device boots, and auto lock after a maximum of 15 minutes of unattended inactivity
   
   ii. Intrusion Prevention- Required- lockout after 25 incorrect attempts within 2 hrs
   
   iii. Encryption- Required-full disk
   
   iv. Remote Wiping- Not applicable

[1] Use of mobile devices to access, store, or manipulate critical information requires:
   
   a) Written approval from the senior executive of the unit involved or the Institutional Review Board confirming a critical business need, and
   
   b) Encrypting the information on the device and in transit.
   
   c) Devices that do not support encryption must not be used to access, store, or manipulate critical information.

B. In addition to appropriate information handling requirements determined by the general data classification, sector-specific date (ex. PCI-DSSs, HIPAA, etc.) may have additional requirements. Check with the appropriate official or office, or contact the UIPO for assistance.
C. Categories of Violations

a) Category 1-Unintentional breach of privacy or security which may be caused by carelessness, lack of knowledge, or lack of judgment. Examples include,
   i. Mistakenly sending e-mails or faxes containing PHI to the wrong recipient
   ii. Leaving a computer accessible and unattended with unsecured PHI
   iii. Loss of an unencrypted electronic device containing unsecured PHI
   iv. Failure to report his/her password has potentially been compromised.

b) Category 2a-Deliberate unauthorized access to PHI without PHI disclosure, such as accessing confidential information of any patient out of curiosity and failure to follow policy without legitimate reason, such as password sharing. Examples include but are not limited to:
   i. Intentional, unauthorized access to your own, friends, relatives, co-workers, public personality’s, or other individual’s PHI (including searching for an address or phone number);
   ii. Fails to properly verify the identity of individuals requesting PHI which results in inappropriate disclosure, access or use of PHI;
   iii. Connects devices to the network and/or uploads software without having received authority;
   iv. Second occurrence of any Category 1 violation (it does not have to be the same offense).

c) Category 2b-Deliberate unauthorized disclosure of PHI or deliberate tampering with data without malice or personal gain. Such as accessing information out of curiosity and then re-disclosure to the news media or unauthorized modification of an electronic document to expedite a process. Examples include but are not limited to:
   i. Intentional unauthorized access to friends, relatives, co-workers, public personality’s or other individual’s PHI and then sharing with news media or on social media;
   ii. Intentionally assisting another individual to gain unauthorized access to PHI. This includes, but is not limited to, giving another individual your unique user name and password to access electronic PHI;
   iii. Changing or tampering with documents for the sole purpose of passing a system edit;
   iv. Second occurrence of any Category 2a violation (it does not have to be the same offense).

d) Category 3-Deliberate unauthorized disclosure of PHI for malice or personal gain. Selling information to tabloids or stealing individually identifiable health information to open credit card accounts. Examples include but are not limited to:
   i. Unauthorized intentional disclosure and/or delivery of PHI to anyone for financial gain;
   ii. Intentionally assisting another individual to gain unauthorized access to PHI for financial gain;
iii. Unauthorized intentional disclosure and/or delivery of PHI to anyone to cause financial and/or reputational harm to embarrassment to the individual;

D. Sanctions

If it is suspected that this policy is not being followed, report the incident to the Department IT manager or representative, Office of Graduate Medical Education, as well as the Chief Information Security Officer.

Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by the provisions of Indiana University Policy IT-02, Policy on Sanctions for Misuse or Abuse of Indiana University Technology Resources. (Reference 5)

6. IMPLEMENTATION

The Designated Institutional Official (DIO) for Graduate Medical Education is responsible for implementation of this policy.

7. OVERSIGHT

Policy authority for this document resides with the Graduate Medical Education Committee. The DIO and the Graduate Medical Education Committee are responsible for oversight. This policy will be reviewed every three years or more often if deemed necessary.

8. REFERENCES

1. **IUSM Security of Mobile Computing Devices**

2. **IU Mobile Devices Security Standard**
   The IU Mobile Devices Security Standard can be found at: [http://protect.iu.edu/cybersecurity/policies/IT12/12.1](http://protect.iu.edu/cybersecurity/policies/IT12/12.1)

3. **IU HIPAA Guidance-Safeguarding Patients’ Photographs and Recording (HIPAA-G02)**
   The IU HIPAA Guidance-Safeguarding Patients’ Photographs and Recording (HIPAA-G02) can be found at: [https://protect.iu.edu/sites/default/files/HIPAA-G02_HIPAA_Guidance_Safeguarding_Patients_Photographs_Recordings.pdf](https://protect.iu.edu/sites/default/files/HIPAA-G02_HIPAA_Guidance_Safeguarding_Patients_Photographs_Recordings.pdf)
4. **VA Wireless Devices Policy**  
See attached.

5. **IU Policy IT-02 Policy on Sanctions for Misuse or Abuse of IU Technical Resources**  
The IU Policy IT-02 Policy on Sanctions for Misuse or Abuse of IU Technical Resources can be found at:  
[http://policies.iu.edu/policies/categories/information-it/it/IT-02.pdf](http://policies.iu.edu/policies/categories/information-it/it/IT-02.pdf)

6. **HIPAA-G01, HIPAA Sanctions Guidance**  
The HIPAA Sanctions Guidance, HIPAA-G01, can be found at:  
Wireless Devices

I. Purpose:

A. To facilitate the needs of medical center users and business partners (government agencies and contractors) for wireless and handheld devices in order to conduct VA business;

B. To define the appropriate care and consideration of wireless services and technologies because they introduce unique vulnerabilities due to their electromagnetic and portable characteristics; and

C. To support the corporate goals of confidentiality, integrity, availability, and accountability of use, of VA systems and information.

II. Policy: VA Employees will use only VA-approved wireless and handheld devices to store, process, transmit, or access VA data and connect to VA Information Systems (IS). Only VA-approved devices, applications, and network/PC connection methods and services will be used in accordance with the below procedures. Business partners, support contractors, and other authorized users that use non-VA-approved wireless and handheld devices to connect to VA systems must use VA approved devices and certify that the devices meet the requirements of this policy. In addition, the devices must be used for business purposes only. Wireless or handheld devices will not be used to process, store, or transmit classified information within the VA unless approved through the CIO and ISO.

III. Implementation:

A. Scope:

1. All VA organizations and Business Partners are directed to follow the policy guidance as closely as possible. In those instances where the guideline cannot be followed because of unacceptable documented consequences to mission, the CIO, ISO or other key official responsible for the system or application in question will request a waiver to this policy from the VA Designated Approving Authority (DAA) and provide an assessment of associated risk and any known mitigation measures.
2. Procedures for securing our wireless devices

B. Procedures:

1. VA Employees will use only VA-approved wireless and handheld devices to store, process, transmit, or access VA data and connect to VA Information Systems (IS). Only VA approved devices, applications, and network/PC connection methods and services will be used in accordance with Paragraph 2.a (4). Approved equipment will be purchased through the PCHS-2 contract.

2. Business partners, support contractors, and other authorized users that use non-VA-approved wireless and handheld devices to connect to VA systems must certify that the devices meet the requirements of this directive.

3. All occupants of federal governed facilities may not install non-VA wireless devices (e.g. Access Points (AP), routers, hubs, & switches).

4. Wireless or handheld devices will not be used to process, store, or transmit classified information within the VA.

5. Wireless technologies (e.g. infrared, acoustic, RF) that store, process, and/or transmit information introduce significant threats to the VA IS due, in part, to unique vulnerabilities of the wireless extensions to the network located outside the physical confines of VA controlled areas. Therefore, the following minimum requirements apply when using wireless devices, services, and technologies with information: (See Appendix A)

   a. Identification and Authentication (I&A). Strong authentication, non-repudiation, and personal identification are required for access to VA IS in accordance with VA security directives. I & A measures will be implemented at both the device and network level.

   b. Confidentiality. Encryption of data transmitted to and from wireless devices is required. The VA DAA is authorized to grant individual exceptions on a case-by-case basis to the requirement for encryption in accordance with VA Information Technology Security Certification and Accreditation Program (ITSCAP).

      (i) Data. Encryption must be implemented end-to-end over an assured channel and will meet the FIPS 140-1 or 2, Overall Level 1 (Triple-DES or AES) standard, at a minimum as required by OMB Circular A-130. [CV1]The detection segment of a PED (e.g., the laser beam between a laser disk and its reader head, between a bar code and the scanner head, or RF energy directed at a passive RF device (paper label tags)) does not require encryption.
(ii) Voice. Voice transmitted over approved cellular carriers does not require encryption unless used to access a voice recognition/synthesis driven data application (e.g., Voice XML).

c. Data Integrity. Wireless devices that store and process information often do not have the same degree of protection afforded by standard desktop operating and file management systems. The VA DAA will require wireless devices to implement file system encryption (where applicable) and ensure that the standard minimum requirements under ITSCAP and other VA security directives are enforced.

d. Availability. Wireless devices are especially vulnerable to denial of service attacks. The VA DAA will ensure measures are taken to mitigate these risks. These risks include not only threats from the outside, but potential interference from friendly sources.

e. Wireless and handheld devices used for storing, processing, and/or transmitting VA data will not be used in areas where classified information is stored, processed, transmitted, or discussed.

f. Wireless devices will not be connected to VA systems for data synchronization, data transfer, or any other purpose without the approval of the VA DAA. Before authorizing connection of wireless devices to VA systems, the DAA will specify risk mitigation strategies such as virus protection, mobile code restrictions, and other preventive measures. In addition, the DAA will insure that detailed guidance on the use of wireless and handheld devices found in VA Handbook 6500 Information Security Program is followed prior to granting connection approval. (It is expected that the VA DAA will usually provide “Type Accreditation” for specific configurations of wireless and handheld devices and services being used within the VA so that each implementation of an accredited wireless or handheld device or service can be used without additional C&A requirements).

g. Upon introduction of wireless technologies, including those creating an external interface to VA systems (or allowing use of VA wireless devices on non-VA wireless networks), the implementing office must renew DAA accreditation of IS operations and will explicitly address the ITSCAP in regard to wireless risk mitigation.

6. Portable Electronic Devices (PEDs)

   a. PEDs include PDAs, cellular/PCS phones, messaging devices, audio/video recording devices, scanners, and hand-held/laptop computers.

   b. PEDs will not be used to store, process, and/or transmit VA data unless adequate security mechanisms are provided to protect the information from compromise as prescribed in 2.a (4).
c. Wireless solutions could create backdoors into VA networks. If a device receives information via a wireless technology and that device allows that information to be placed directly into the VA network at the workstation level, then all perimeters and host-based security devices have been bypassed. Therefore the following procedures apply:

(i) PEDs that are connected directly to a VA wired network (e.g., via a hot synch connection to a workstation) would not be permitted to operate wirelessly at the same time.

(ii) Ad-hoc connections using an IR, Bluetooth or 802.11 peer-to-peer communications could be used to pass malicious code into the device while it isn’t in the cradle. The device could then be commanded to extract information from the VA network when it is placed in the cradle for later recovery. IR, Bluetooth, and 802.11 peer-to-peer communications capabilities will be set to off as the device default setting.

(iii) Mobile code will not downloaded from non-VA sources. Downloading of mobile code will only be allowed from trusted VA sources over assured channels.

(iv) The use of VA-approved anti-virus software on PEDs and workstations that are used to synchronize/transmit data is mandatory, if available. Where antivirus software is not yet available for a device, disabling the synchronization capability or providing server or workstation based handheld antivirus protection is required. To ensure consistent levels of protection required against viruses, PED users will maintain up-to-date anti-virus signature files on their PED.

(v) PEDs are easily lost or stolen. To protect against loss of sensitive information, Protected Health Information (PHI) and electronic Protected Health Information (ePHI) the use of VA-approved file system/data store encryption software on PEDs is mandatory, if available.

(vi) PEDs will be capable of being erased/zeroized/overwritten. If PEDs that were used to store, process, and/or transmit VA data are deemed no longer needed, and cannot be erased/zeroized/overwritten to the satisfaction of the VA DAA, they will be physically destroyed in a manner that ensures that stored data is not recoverable.

(vii) PEDs that support the wireless application protocol (WAP) and utilize commercial wireless network providers are at risk for information compromise. Data will not be transmitted in this situation unless it can be ensured that data is encrypted end-to-end using a FIPS 140-1/2 Level 1 approved encryption algorithm.

(viii) The Air Fortress Secure Client is a software client module for securing laptops, PDAs, and tablets PC’s and shall be installed on all PEDs
requiring wireless network access. This client is required for devices to communicate with networks protected by the Air Fortress Wireless Security Gateway.

d. PED systems will be configured according to the guidance in Appendix B.

7. Cellular/PCS and Wireless Email

(i) Cellular/PCS and wireless email devices are subject to several vulnerabilities (e.g. interception, scanning, remote command to transmit mode, etc). Therefore cellular/PCS and wireless email devices that are used to transmit VA information will only be used when specifically approved by the VA DAA.

(ii) Cellular/PCS and wireless email devices will not be allowed into an area where classified information is being discussed unless it is rendered completely inoperable. Turning off a Cellular/PCS & wireless email device may not prevent remote activation on a device having a sleep mode.

(iii) Wireless email services will provide end-to-end encryption in accordance with Paragraph 2.a(4)(b). VA email will be “redirected” to the wireless device by server based redirectors only. PC based redirectors are prohibited from use because they require the users network logon and email service to be active at all times.

(iv) VA employees that use the Blackberry wireless email service will follow the Blackberry configuration guidance in Appendix C.

8. Synchronization

(i) Synchronization of wireless and handheld devices with applications or data located on a VA workstation or server (e.g. Microsoft Outlook) via a “hot-sync” cable or cradle can expose VA IS to significant security risks. Some synchronism systems will operate even if the workstation is locked and the wireless or handheld device is not registered with the synchronization application on the workstation. As long as the workstation is on, the user is logged on, the data application client (e.g. MS Outlook) is active, and the “hot-sync” cable is attached to the workstation any person can place a compatible wireless or handheld device in the “hot-sync” cradle and download data. Therefore the procedures found in Appendix B and Appendix C applies.
IV. References:

A. VA Wireless Guidance dated 07-17-02.
   B. NIST_SP_800-48.
   
   C. VA Directive 6500, Information Security Program


Thomas Mattice
Medical Center Director

Attachments:
   Appendix A, Wireless LAN(s) Configuration
   Appendix B, PDA Security/Configuration
   Appendix C, Blackberry E-Mail Security Configuration
Certification

I understand the requirements set forth in the HIPAA Privacy and Security Rules and the Final Rule of the HITECH Act and related state laws for using and/or disclosing protected health information (PHI). I also understand my responsibilities under those regulations as well as my responsibilities under the IU HIPAA Privacy and Security Compliance Plan.

I own the following digital devices, but have never used them to access or store PHI, nor will I do so in the future without first ensuring that the device is encrypted and has strong password protection:

__________________________________  __________________________________
__________________________________  __________________________________
__________________________________  __________________________________

I own the following digital devices and have used them to access or store PHI, and hereby agree to allow IU to conduct testing on the device(s) to ensure that they are encrypted and have strong password protection. I understand that I will not be permitted to engage in clinical activities if I decline to allow my device(s) to be tested.

__________________________________  __________________________________
__________________________________  __________________________________
__________________________________  __________________________________

I understand access includes but is not limited to viewing information in Cerner, CareWeb, a research data base of spreadsheet and/or an IU email account.

____________________________________________  _________________________
Signature  Date

____________________________________________
Printed Name

IU School of Medicine, Department of _________________________