INDIANA UNIVERSITY
SCHOOL OF MEDICINE

Data Security on Mobile Devices

gme-adm-0030

About This Policy

Effective Dates:
11-13-2013

Last Updated:
10-25-2023

Responsible University Administrator:
Senior Associate Dean for GME

Policy Contact:
GME Assistant Director

Scope

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

Policy Statement

Any mobile computing device that is used to access institutional data or PHI is subject to all Indiana University (IU), IUSM, and affiliate covered entity policies. This includes personally-owned devices.

Information stored on and accessed from mobile computing devices is potentially at risk of inappropriate exposure due to loss, theft, and cybersecurity incidents. Therefore, safeguards must be applied to mobile computing devices that are used to store and to access institutional data or PHI.

When working within an affiliate covered entity which is not part of IU, residents must comply with the policies and procedures of that covered entity (see references). Residents must follow institutional and departmental policies that define appropriate configuration and use of institutionally sanctioned software designed for accessing PHI.

At IUSM, PHI may only be stored in IT services and systems approved for critical data.

Reason For Policy

The purpose of this policy is to define mobile computing device requirements needed to protect institutional data and Protected Health Information (PHI) that may be stored on or accessed from such devices.

Procedure

Please review the “IU Mobile Devices Security Standard” policy using the link under Related Information.

Definitions

ACGME is the Accreditation Council for Graduate Medical Education.

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.

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.

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.*

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.*

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.

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

PCI-DSS – is the **P***ayment* **C***ard* **I***ndustry* (PCI) **D***ata* **S***ecurity* **S***tandard* (DSS).

PHI – is protected health information.

UIPO – is the Indiana University Information Policy Office.

Sanctions

Suspicious incidents that may not comply with this policy should be reported to the department IT manager or representative, Office of GME, and 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*.

Implementation

The Designated Institutional Official (DIO) for GME is responsible for implementation of this policy.

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.

History

1. Policy IUSM-GME-PO-0029 approved by GMEC and published on 13 November 2013.
2. Policy reviewed, updated, and approved by GMEC on 13 November 2013.
3. Policy reviewed, updated, and approved by GMEC on 28 February 2018.

4. Policy updated for formatting 05 March 2018.
5. Policy reviewed by Polices & Procedures Subcommittee 18 June 2018.
6. Policy updated for formatting 27 June 2018.
7. Policy updated 16 October 2023.
8. Policy renamed to gme-adm-0030 and published to the IUSM policy portal on 19 August 2024.