INDIANA UNIVERSITY

HIPAA-P08
Removal and/or Transport of Protected Health Information

FULL POLICY CONTENTS

Effective: July 1, 2014
Last Updated: August 1, 2016

Responsible University Office:
HIPAA Privacy and Security Office

Responsible University Administrator
Vice President for University Clinical Affairs

Policy Contact:
University HIPAA Privacy Officer
University HIPAA Security Officer

Scope

This policy applies to all personnel, regardless of affiliation, who have access to Protected Health Information ("PHI") under the auspices of Indiana University, designated for purposes of complying with the final provisions of the security and privacy rules regulated by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Please refer to the HIPAA Affected Areas document for a full list of units impacted within Indiana University.

This policy addresses transportation or removal of PHI from the workplace.

Reason for Policy

Members of the IU HIPAA Affected Areas workforce who are tasked with the transportation of sensitive information from location to location or are assigned to work from home part-time, full-time or on an exception basis in an official IU capacity are responsible for maintaining the privacy and security of all Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) and for following all IU policies and procedures related to Critical Data, PHI, and ePHI.

Indiana University (IU) has a legal and ethical responsibility to maintain the confidentiality, privacy and security of all PHI it creates, receives or maintains. This policy is to ensure appropriate safeguards against the lost, theft, and unauthorized access, use, disclosure, alteration or destruction of protected health information and personal information in paper form or stored in electronic form or laptops or USB drives by providing basic requirements for the physical removal or transport of such information from or within our institution.

Definitions

See HIPAA Glossary for complete list of terms.

Policy Statement

I. Permission and Conditions

A. Workforce members shall not physically remove or transport any PHI, or PI from IU Work Locations, unless such information will be used for the performance of their job duties and in compliance with this policy.

B. Workforce members shall ensure that all PHI and PI, whether in paper or electronic format, that is physically removed from IU Work Locations for their job duties is secured and transported in compliance with this policy and referenced policies.

C. Workforce members must have written prior approval from an authorized University Official (immediate supervisor, director, chair, PI, Dean) prior to transporting or removing PHI or PI from an Indiana University Work Location.

D. Workforce members who may transport or remove PHI or PI must have a signed *Confidentiality Agreement* on file in their respective IU HIPAA Affected Area.

II. Removal:

A. Workforce members shall not remove any original paper medical records from their IU Work Location except to transport between IU Work Locations.

B. *Electronic*: Workforce members shall not physically remove any PHI or PI stored in electronic form on laptops or USB devices from IU Work Locations unless the laptop or USB device on which it is stored is in compliance with all applicable IU encryption policies and standards. (IU Policy IT-12.1)

C. *Paper:* Workforce members shall not remove PHI or PI in non-electronic form (whether originals, copies, replications, or reproductions) from IU Work Locations, except to transport between such spaces, unless one of the following specific exceptions apply:

Exceptions:

1. The workforce member has received approval from his/her immediate supervisor or the director in the department where he/she works, or, in the case of research activities, from the Principal Investigator, for the purpose of performing work offsite in accordance with the policy set forth in Section 4 below; or

2. The workforce member requires access to PHI or PI offsite to perform activities related to the provision of patient care.

III. Transport

A. Workforce members who transport PHI or PI in any form, and whether on-site or off-site, shall take reasonable precautions to safeguard and secure the information at all times.

B. Workforce members shall only transport the minimum information necessary to perform their job duties.

C. Workforce members shall transport information so that it is not viewable or accessible to others (e.g. brief case, locked canvas bag, etc.).

D. Workforce members shall not take home PHI or PI they are transporting between IU Work Locations.

E. All transport personnel in various departments shall adhere to department specific procedures.

F. Workforce members shall not leave PHI or PI publicly unattended or unsecured at any time.

IV. Process to request transport or removal of PHI

A. Workforce members who seek to take non-electronic PHI or PI from IU Work Locations to work at home or offsite must request approval from their supervisor or the department's director and, in the case of research activities, from the Principal Investigator.

B. Before approving the request, the supervisor, director or PI shall be satisfied that the workforce member will implement proper safeguards for protecting the information when physically removed from Indiana University Work Locations.

Sanctions

Workforce members who violate this policy are subject to sanctions up to and including termination from employment.

The workforce member and the supervisor/director who authorized the removal of information may be subject to corrective action, up to and including termination as applicable, if PHI or PI removed from IU Work Locations are not appropriately safeguarded as provided in this policy.

Related Information

HR	Telecommuting Guidelines for Non-emergency Situations
IT-12.1	IU Mobile Device Security Standard
HIPAA-A02	General Administrative Requirements

HIPAA-G01	HIPAA Sanctions Guidance
HIPAA-P01	Uses & Disclosures of Protected Health Information Policy
HIPAA-P02	Minimum Necessary Policy

History

11/12/13	Draft Sent to HIPAA Privacy and Security Compliance Council
07/01/2014	Final
08/01/2016	Updated Definitions Section.