Removal and/or Transport of Protected Health Information

HIPAA P-08

About This Policy

Effective: *July 1, 2014*
Last Updated: *September 1, 2021*

Responsible University Office:
Office of the Chief Privacy Officer

Responsible University Administrator:
Chief Privacy Officer
mawerlin@iu.edu

Policy Contacts:
HIPAA Privacy Officer
HIPAA Security Officer
hipaa@iu.edu

Scope

This policy applies to the workforce members in the designated Indiana University (IU) HIPAA Covered Healthcare Components and HIPAA Affected Areas, anyone rendering services as a Business Associate, and anyone who creates, receives, maintains, or transmits Protected Health Information (PHI) in any capacity at IU, including, but not limited to, faculty, staff, students, trainees, volunteers, visiting scholars, and third-party agents. For the purposes of this policy, all of the above will be referred to as workforce members.

Policy Statement

A. Workforce members shall not physically remove or transport any PHI from IU work locations unless such information is necessary for the performance of their job duties and in compliance with this policy.

B. Workforce members must have approval from their supervisor or Principal Investigator (PI), when engaged in research activities, prior to removing or transporting PHI from an IU work location. Before approving the request, the supervisor or PI must ensure the workforce member has the proper resources for safeguarding the PHI. The approval shall be documented and retained by the workforce member.

C. Workforce members shall ensure that all PHI, whether in paper or electronic format, that is physically removed from IU work locations is the minimum information necessary for their job duties and is secured and transported in compliance with this policy and referenced policies and guidelines.

D. Workforce members shall not remove any original paper medical records from their IU work location except to transport between IU work locations necessary for their job duties.

E. Workforce members shall not physically remove any PHI stored in electronic form on mobile devices from IU work locations unless the device on which it is stored is in compliance with all applicable IU encryption policies and standards. (IU Policy IT-12.1)

F. Workforce members who transport PHI in any form, and whether on-site or off-site, shall take reasonable precautions to safeguard and secure the information at all times. (See Attachment 1, Guidelines for the removal and transport of PHI)

Reason for the Policy

Members of the IU workforce who are tasked with the transportation of PHI 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 the PHI and for following all IU policies and procedures related to HIPAA and Critical Data.

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 loss, theft, and unauthorized access, use, disclosure, alteration or destruction of PHI in paper form or stored in electronic form on mobile devices by providing basic requirements for the physical removal or transport of such information from or within IU.

Definitions

Individually Identifiable Health Information (IIHI): 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 identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information (PHI): Individually identifiable health information held or transmitted by a covered entity or its business associate in any form or medium, whether electronic, on paper or oral.

See Glossary of HIPAA Related Terms for complete list of terms.

Sanctions

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

History

07/01/2014 Effective Date
08/01/2016 Updated Definitions Section, added link to Glossary
06/01/2017 Published on University policy site
10/31/2018 Updated Section 2C
09/01/2021 Updated contacts and revised for remote work arrangements

Related Information

Human Resources Remote Work Guidance
HIPAA-P02 Minimum Necessary Policy
IT-12.1 IU Mobile Device Security Standard
ACA-83 Remote Work for Academic Appointees
HR-06-80 Remote Work for Staff and Temporary Employees

OFFICE OF THE
CHIEF PRIVACY OFFICER

Guidelines for the removal and transport of PHI

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

The following safeguards shall be implemented to protect against the loss, theft, unauthorized access, use, disclosure, alteration or destruction of protected health information.

- Department Lead shall approve and accept any risks associated with the removal and transport of PHI for telecommuting purposes.
- Supervisor or Principal Investigator shall approve an individual's request and specific documents to be removed.
- The individual requesting to remove documents containing PHI shall confirm their home environment can be appropriately managed to ensure the privacy and security of the documents.
- HIPAA Privacy and Security Training must be up-to-date prior to an individual removing PHI.
- The documents (charts, binders, etc.) assigned to each individual being removed, must be logged out and logged back in upon return.
- The number of documents logged out by an individual shall be limited and only the minimum necessary needed to perform the job duties.
- The data elements contained on the documents shall be noted.
- Two individuals should be present while logging out and logging in documents to ensure the correct documents have been taken/returned. The log shall be signed by the individual and the witness.
- During transport, charts should be in a locked container or a sealed envelope/box and not carried loosely offsite and viewable or accessible to others.
- Documents are never to be left in an unattended vehicle.
- Documents are never to be brought into a public location (Starbucks, etc.).
- Documents are to remain in the possession of the staff member at all times during transport and should be transported directly from the school office to the home office, i.e. not left in the car to run an errand or overnight.
- Secure documents at home when not in use by returning to the locked container or envelope/box.
- The integrity of the documents are to be maintained while off site.
- Any incident involving the privacy or security of documents containing any restricted or critical data is to be reported immediately to it-incident@iu.edu.
- Departments that transport documents containing PHI during their regular course of business may comply with the HIPAA P-08 policy by continuing to follow the department's established protocols.

Contact: HIPAA Privacy Officer, 812-856-0340, hipaa@iu.edu