Electronic Communications and Protected Health Information HIPAA P-10

About This Policy

Effective: 08/01/2017
Last Updated: 04/07/2025

Responsible University Office:
Office of the Chief Privacy Officer

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

Policy Contact:
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 Critical Health Data 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.

This policy **does not** address patient-physician electronic communication pertinent to the ongoing care of the patient, as well as other patient-related electronic communications, that must be maintained as part of, and integrated into, the patient's medical record, whether that record is paper or electronic. Healthcare providers must comply with Indiana Administrative Code: 844 IAC 5-3, Appropriate Use of the Internet in Medical Practice.

All Indiana University faculty, staff, residents, and fellows must comply with the policies and procedures of the respective covered entity when working within a covered entity which is not part of Indiana University. All Indiana University students must comply with the policies and procedures of the respective covered entity when the students' clinical experience is within a covered entity which is not part of Indiana University.

Policy Statement

A. Security Requirements

Workforce members must comply with the following security requirements whenever Individually Identifiable Health Information/Protected Health Information (IIHI/PHI) is included in an electronic message:

1. The use or disclosure of IIHI/PHI must be permitted per the HIPAA Privacy Rule and IU policy, HIPAA-P01 – IU Uses and Disclosures of PHI;
2. Electronic messages containing IIHI/PHI may not be sent or received except with a device that has been secured in compliance with, as applicable, IU IT-12, IT-12.1 policies;
3. IIHI/PHI must be limited to the minimum information necessary for the permitted purpose per the HIPAA Privacy Rule and IU policy, HIPAA-P02 – Minimum Necessary;

4. Highly sensitive IIHI/PHI (e.g. mental health, substance abuse, or HIV information) should be transmitted by electronic messaging **only in** exceptional circumstances;
5. IIHI/PHI may only be sent by electronic messaging after the recipient's contact information (e.g. email address or cell phone number) has been carefully verified and entered correctly;
6. Electronic messages containing IIHI/PHI should be deleted as soon as possible and should not be "stored" or "archived" in email folders or on a mobile device. *If the message is related to treatment, the message may need to become part of the patient's medical record, which is not addressed in this policy.*
7. IIHI/PHI may never be sent through an Instant Messaging (IM) program (e.g. IM through Skype for Business or Lync).

B. Email (electronic mail)

1. Email usage:
    a. IU personnel must use an IU Exchange email account or your IU affiliate's Exchange email account to send and receive IIHI/PHI, and may never use personal email accounts (e.g. Google or Yahoo accounts) for that purpose;
    b. IU Exchange email accounts that may send or receive IIHI/PHI may never be auto-forwarded to a personal email account;
    c. Email messages containing IIHI/PHI should not be forwarded to other users, unless there is a documented business need to do so.
2. Encrypted/Secure email messages:
    a. All emails containing IIHI/PHI must be encrypted unless the message meets an exception in Section II.C.
    b. User(s) must use Office Message Encryption (OME) to encrypt certain sensitive data when it leaves the IU network.
3. Exceptions to OME:
    a. Communication between IU personnel using IU's Exchange Server.
    IU personnel on the IU Exchange server may send unencrypted email messages containing IIHI/PHI when communicating with other IU personnel on the IU Exchange server provided:
        i. The security measures set out in Section I are followed;
        ii. The email remains on IU's Exchange Server;
        iii. The connection to the system is secure;
        iv. The message includes **Confidential** at the top of the body of the message, to identify IU believes this record meets an exemption under the Indiana Access to Public Records Act (APRA), IC § 5-14-3.
    b. Communication from IU personnel on IU's Exchange Server to IU affiliate hospital system including (1) IU Health; (2) IU Health Physicians; (3) Eskenazi Health; and/or (4) Regenstrief Institute.
    IU personnel on the IU Exchange server may send unencrypted email messages containing IIHI/PHI when communicating with individuals who have IU Health, Eskenazi or Regenstrief email addresses provided:
        i. The security measures set out in Section I are followed;
        ii. The email remains on an Exchange Server;
        iii. The connection to the systems are secure;
        iv. The message includes **Confidential** at the top of the body of the message, to identify IU believes this record meets an exemption under the Indiana Access to Public Records Act (APRA), IC § 5-14-3.
    c. Communication from IU personnel on IU's Exchange Server to patients or research subjects. IU personnel may send unencrypted email messages containing IIHI/PHI to patients and/or research subjects provided:
        i. The security measures set out in Section I are followed;

ii. The patient, research subject or their representative has been advised of the inherent risks associated with sharing IIHI/PHI via unsecured electronic communication;
iii. The patient, research subject or their representative has consented to the use of unsecure email messages by completing a version of the "Indiana University Authorization for Unsecure Electronic Communication" form. The form must include:
    - The risks of using unsecured electronic communication; and
    - The specific purpose or use of the electronic communication (e.g. appointment reminders, reminder of research tasks, scheduling reminders).

ii. The message includes **Confidential** at the top of the body of the message, to identify IU believes this record meets an exemption under the Indiana Access to Public Records Act (APRA), IC § 5-14-3.

C. Text Message

1. IU does not have an approved secure or encrypted method to share IIHI/PHI via text message.
2. All text messages containing IIHI/PHI must meet the security requirements established in Section I.
3. Secure Text messages may be sent using a service approved by one of IU's affiliated organizations (e.g. IU Health, Eskenazi, VA), if applicable.
4. Unsecure Text messages to patients or research subjects can only occur if:
    a. The patient, research subject or their representative has been advised of the inherent risks associated with sharing IIHI/PHI via unsecured electronic communication;
    b. The patient, research subject or their representative has consented to the use of unsecure email messages by completing a version of the "Indiana University Authorization for Unsecure Electronic Communication" form. The form must include:
        i. The risks of using unsecured electronic communication; and
        ii. The specific purpose or reason for the electronic communication (e.g. appointment reminders, reminder of research tasks, scheduling reminders).

D. Misdirected Electronic Messages

1. Misdirected Emails or Text Messages should be treated as an incident.
2. **Comply with IU ISPP-26,** Information and Information System Incident Reporting, Management, and Breach Notification.

Reason for the Policy

Indiana University is committed to protecting the privacy and security of health information as required under the HIPAA Privacy and Security Rules. The purpose of this policy is to establish administrative, technical, and physical safeguards to protect the privacy and security of electronic communication (e.g. email, text messages) that may contain protected health information and to establish guidelines for communication with Indiana University patients and/or research subjects that complies with state and federal laws.

HIPAA allows covered entities and their business associates to communicate ePHI with patients via email and text message if: (1) the emails and texts are encrypted and/or are otherwise secure; or (2) the covered entity or business associate first warns the patient that the communication is not secure and the patient elects to communicate via unsecure email or text message, anyway. When it comes to communicating with non-patients, the covered entity or business associate must generally ensure that its email or texts comply with relevant Privacy and Security Rule standards.

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.

Minimum Necessary: A standard that requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does not apply to certain uses or disclosures such as those requests by a health care provider for treatment purposes, disclosures to the individual who is the subject of the information or pursuant to an individual's authorization.

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.

History

08/01/2017 – Effective Date
05/19/2020 – Updated method to force encryption through CRES
12/13/2021 – Updated policy contacts
04/07/2025 – Updated terms

Related Information

Indiana Law
IC § 5-14-3: Indiana Access to Public Records Act (APRA)
844 IAC 5-3: Appropriate Use of the Internet in Medical Practice.