INDIANA UNIVERSITY

HIPAA–P10
Electronic Commuication and PHI Including Emails and Text Messages

FULL POLICY CONTENTS

Effective: August 1, 2017
Last Updated: May 19, 2020

Responsible University Office:
Office of the Chief Privacy Officer

Responsible University Administrator
Chief Privacy Officer

Policy Contact:
University HIPAA Privacy Officer

Scope

This policy applies to all IU personnel, regardless of affiliation, who intend to use electronic communication (e.g. email, text message) as a way of sharing individually identifiable health information (IIHI) and/or protected health information (PHI), as both are defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), under the auspices of Indiana University. This policy is designated for the purpose of complying with the final provisions of the privacy and security rules regulated by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

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. Physicians 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.

Reason for 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

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

Policy Statements

I. Security Requirements

IU HIPAA Affected Areas or IU workforce members must comply with the following security requirements whenever IIHI/PHI is included in an electronic message:

A. 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;
B. 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;
C. 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;
D. Highly sensitive IIHI/PHI (e.g. mental health, substance abuse, or HIV information) should be transmitted by electronic messaging **only in** exceptional circumstances;
E. 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;
F. 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.*

G. IIHI/PHI may never be sent through an Instant Messaging (IM) program (e.g. IM through Skype for Business or Lync).

II. Email (electronic mail)

A. Email usage:

1. 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;
2. IU Exchange email accounts that may send or receive IIHI/PHI may never be auto-forwarded to a personal email account;
3. Email messages containing IIHI/PHI should not be forwarded to other users, unless there is a documented business need to do so.

B. Encrypted/Secure email messages:

1. All emails containing IIHI/PHI must be encrypted unless the message meets an exception in Section II.C.
2. User(s) must enter **[Secure Message]** (case insensitive, with square brackets) in the subject line of the email to force encryption through the IU Cisco Registered Envelope Service (CRES). More information on CRES may be found here: https://kb.iu.edu/d/bbtq.

C. Exceptions to CRES encryption:

1. 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:
   a. The security measures set out in Section I are followed;
   b. The email remains on IU's Exchange Server;
   c. The connection to the system is secure;
   d. 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.
2. 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:
   a. The security measures set out in Section I are followed;
   b. The email remains on an Exchange Server;
   c. The connection to the systems are secure;
   d. 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.
3. 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:

a. The security measures set out in Section I are followed;
b. The patient, research subject or their representative has been advised of the inherent risks associated with sharing IIHI/PHI via unsecured electronic communication;
c. 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 use of the electronic communication (e.g. appointment reminders, reminder of research tasks, scheduling reminders).
d. 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.

III. Text Message

A. IU does not have an approved secure or encrypted method to share IIHI/PHI via text message.
B. All text messages containing IIHI/PHI must meet the security requirements established in Section I.
C. 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.
D. Unsecure Text messages to patients or research subjects can only occur if:
    1. The patient, research subject or their representative has been advised of the inherent risks associated with sharing IIHI/PHI via unsecured electronic communication;
    2. 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:
        a. The risks of using unsecured electronic communication; and
        b. The specific purpose or reason for the electronic communication (e.g. appointment reminders, reminder of research tasks, scheduling reminders).

IV. Misdirected Electronic Messages

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

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.

History

08/01/2017	Effective Date
05/19/2020	Updated method to force encryption through CRES