2021 Annual Training

Regenstrief Institute
Better Care. Better Health.

INFORMATION SECURITY AND PRIVACY AWARENESS

In this document:

HIPAA Training

The Institute's annual HIPAA training is conducted on the CITI website.

You may complete the Institute's HIPAA training by either completing the CITI training or by providing a certificate of completion from another organization's CITI training.

All 13 modules within the course must be completed with an average quiz score of at least 80%.

"When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else."
— David Brin

Objective

Regenstrief Institute is required to protect the privacy and confidentiality of Personally Identifiable Information (PII) and Protected Health Information (PHI) whenever it is used by staff, faculty, contractors, and volunteers. This document summarizes Institute and Indiana University-specific information not included in the information security training on CITI.

HIPAA Compliance Officer

Regenstrief has designated the Privacy and Compliance Officer as the HIPAA privacy officer, and any questions or issues regarding protected health information should be presented to the Privacy and Compliance Officer.

Email the Privacy and Compliance Officer at mckinlec@regenstrief.org if you have any questions about privacy, HIPAA, PHI/PII, or this document.

Indiana University Resources

See the website https://protect.iu.edu/index.html for more information about IU information security and privacy policies and training resources.

Health Technology Services (HTS) provides the Institute's information technology support and infrastructure. HTS can be contacted at (317) 274-5336 or htshelp@iu.edu.

Regenstrief Institute
Better Care. Better Health.

EthicsPoint

ANONYMOUS REPORTS

https://www.regenstrief.ethicspoint.com

Anyone may make an anonymous or identifiable ethical, information security or privacy report on EthicsPoint.

Protecting PHI or PII

The preferred method of storing PHI is using Microsoft Secure Storage at IU.

At Indiana University, through a combination of account and folder configurations, Microsoft Secured Storage at IU can be used for Restricted and some Critical institutional data, such as PHI or PII.

Information about Microsoft Secured Storage at IU can be found at https://kb.iu.edu/d/bgfb

Other Approved Storage

- IU REDCap
- IU Karst enclave
- IU OnCore
- Regenstrief Institute servers
- Other enterprise storage solutions approved for storing PHI or PII.

Not all storage locations are acceptable for critical information. Critical information in electronic format must be professionally secured to prevent it from being compromised or stolen.

PHI or PII may be destroyed by:

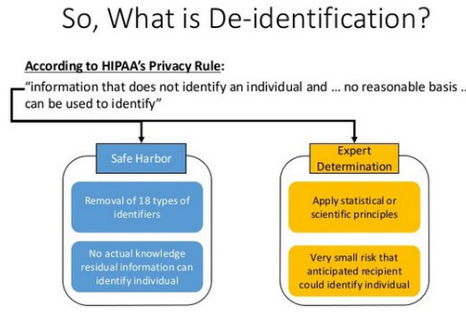
- Placing paper documents into the GRM containers for shredding.
- Deleting electronic PHI or PII and removing from the Windows Recycle folder.
- Physical electronic storage media must be either wiped using an approved disk wiping utility or destroyed by the IU Surplus Data Destruction Service.
- See IU's Secure Data Removal information at https://protect.iu.edu/online-safety/protect-data/data-removal.html.

Regenstrief Institute
Better Care. Better Health.

De-Identifying PHI or PII

PHI or PII may be de-identified by:

1. Requesting a Data Core Honest Data Broker to de-identify your data set; or
2. Requesting the Privacy and Compliance Officer to review and approve your de-identification.



EMAIL

Forwarding Emails and IU Exchange

No one may automatically forward emails from their IU Exchange account to a private email server (Gmail, Yahoo!, etc.).

Automatically forwarding emails to a private email server increases the likelihood of a data breach.

All Institute business should be conducted using a faculty or employee IU Exchange account.

NEAR MISSES

Emails containing PHI are the Institute's primary cause of privacy and compliance near misses.

SECURITY BREACH

Possible Breaches

- Emailing PHI or PII to the wrong recipient.
- Discussing PHI or PII on social media.
- Placing PHI or PII in a Power-Point slide.
- Faxing PHI or PII to the wrong recipient.
- Losing paper records containing PHI or PII
- Losing a flash drive containing PHI or PII.
- Losing a laptop containing PHI or PII.

Got a Breach?

Don't panic.

As soon as possible, contact the Privacy and Compliance Officer and submit a report in EthicsPoint.

In the Remote Work Setting remember:

1. Do not discuss PHI with others present.
2. Ensure any documents with PHI are stored in secured locations.
3. Ensure that you are using VPN when accessing PHI.
4. Ensure your home internet connection is secured with a password.
5. Lock your work station when you walk away, even while at home.

Regenstrief Institute
Better Care. Better Health.

PHISHING

See the website https://protect.iu.edu/index.html for more information about phishing education and training.

Forward suspected phishing emails with full headers to phishing@iu.edu.

For instructions on displaying and sending emails with full headers, see https://kb.iu.edu/d/adix.

MS Outlook users can install the PhishMe Reporter add -in for Windows or Mac to report phishing attempts with a single click. See https://kb.iu.edu/d/aogv for more information about PhishMe.

COMMON SENSE RULES

Institute systems and networks are for business purposes only.

Occasional personal use is permitted so long as the use does not impair your work or affect business systems and networks.

What is considered "occasional personal use" of Institute systems and networks is determined solely by Institute management.

Do not use Institute systems or networks for viewing or accessing questionable content or conducting unlawful activity.

Report inappropriate use of Institute systems or networks to your supervisor make an anonymous report on EthicsPoint.