Regenstrief Institute

Information Security and Privacy Awareness Mandatory Training

December 2024 – December 2025

In this training we will cover:

- HIPAA Issues
- Privacy, Compliance and Security Officer Roles
- IU Resources
- Rules for PHI/PII
- How to Make Reports
- Common Sense Rules

HIPAA Training

The Institutes annual HIPAA training is conducted on the CITI website.

You will complete the Institute's HIPAA training by completing the CITI training associated to Regenstrief or by providing a certificate of completion from another organization's CITI Training.

You must complete all 13 modules within the CITI course 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

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 training summarizes Institute and Indiana University-specific information not included in the information security training on CITI.

Privacy, Security and Compliance Officers

Regenstrief Institute has a designated the following roles:

Compliance Officer: Joyce Hertko (jhertko@regenstrief.org)
Ensures adherence to legal, regulatory, and ethical standards by developing compliance programs, conducting audits, and training employees.

Privacy Officer: Karen Crow (crowk@regenstrief.org)
Safeguards sensitive information by developing privacy policies, monitoring compliance, investigating privacy issues, and educating staff on privacy practices. Serves as the designated HIPAA Privacy Officer.

Information Security Officer: Tony French (adfrench@egenstrief.org)
Protects information systems by developing security policies, conducting risk assessments, managing incidents, and providing security training on best practices. Serves as the designated HIPAA Security Officer.

Information Security and Privacy Policies

Regenstrief staff, faculty and community members are required to review and be familiar with Regenstrief Institute Information Technology and Privacy & Compliance policies, procedures, and standards published under the Library section of the Regenstrief Institute Intranet, including but not limited to:

- **Acceptable Use Policy**
- **Acceptable Use Agreement**
- **Data Management and Use Policy**
- **Incident Reponse Policy**
- **Incident Reporting Procedures**
- **IT Procurement Policy**
- **Master Information Security Policy**
- **Mobile Device Security Policy**

Information Security Incident Reporting

Immediately report any suspected or actual security incidents of information, abnormal systematic unsuccessful attempts to compromise information, or suspected or actual weaknesses in the safeguards protecting information - whether in printed, verbal, or electronic form – or of information systems used in the pursuit of the Institute's mission.

Regenstrief Institute Information Security

- Email: riisec@regenstrief.org,
- Phone: 317-274-9443

Emergency IT incidents *may be reported directly to University Information Security Office (UISO) but must also be reported to Regenstrief Institute Information Security who will then coordinate the response:* https://informationsecurity.iu.edu/report-incident/emergency-it-incidents.html

Potential HIPAA, or ethics violations should also be reported to EthicsPoint:

- Web: https://regenstrief.ethicspoint.com/
- Phone: 844-449-7488

ANONYMOUS REPORTS

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

Regenstrief Institute
www.regenstrief.org

Indiana University Resources

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

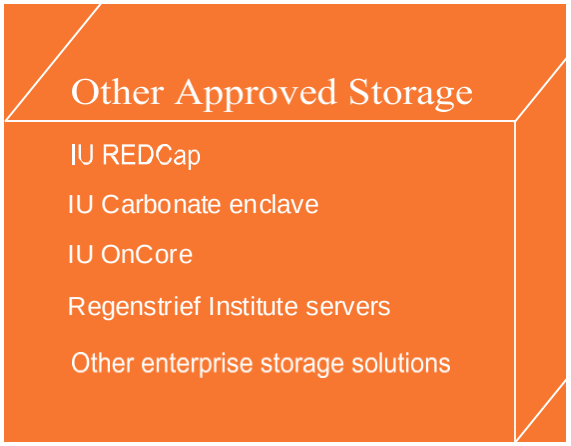
Health Technology Services (HTS) provides the Institute's information technology support and infrastructure. HTS can be contacted at (317) 274-5336 or htshelp@iu.edu

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://servicenow.iu.edu/kb?id=kb_article_view&sysparm_article=KB0025537



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.

Regenstrief Institute
www.regenstrief.org

Protecting PHI or PII (cont.)

Guidelines for devices:

- Regenstrief-issued or registered devices **must** be used for accessing Regenstrief systems and/or data, except for limited communication tools such as Outlook/Exchange, Slack, Teams, and Microsoft 365.
- Critical information, including PHI, **may not be stored** on local devices, including Regenstrief or IU-issued desktops, laptops, phones, tablets, other mobile devices, or external devices such as thumb drives. Approved secure storage options must be used for critical information.
- Critical information, including PHI, **may not be accessed and/or manipulated** using mobile devices, unless these devices meet the provisions under the Mobile Device Security Policy.

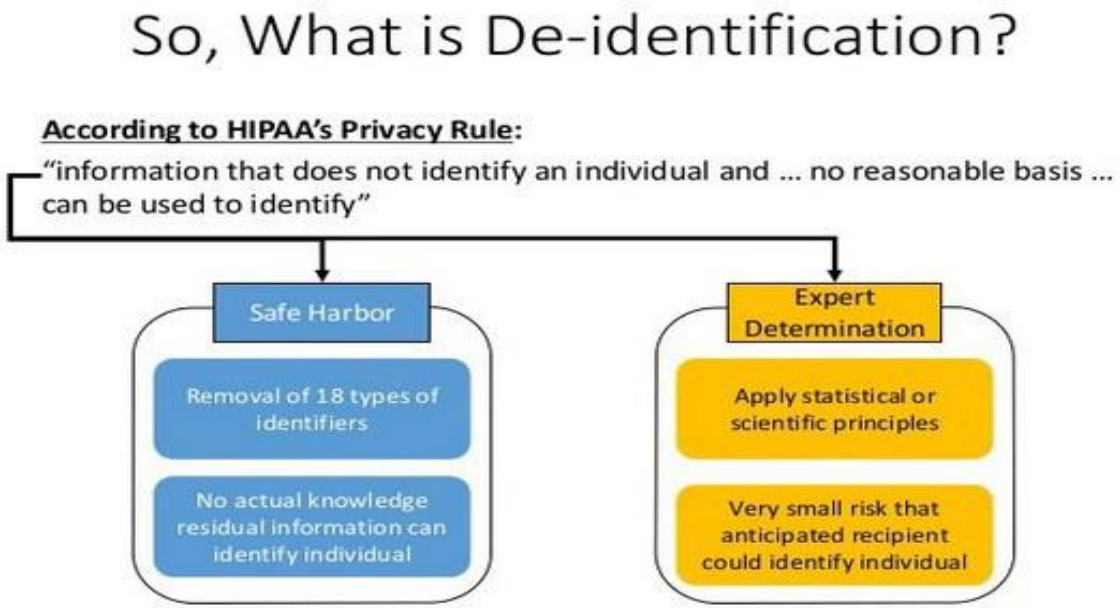
- For more information, see the Mobile Device Security Policy and IU's Knowledge Base Article, "Protect data on your mobile device".

Protecting PHI or PII (cont.)

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://servicenow.iu.edu/kb?id=kb_article_view&sysparm_article=KB0025426.

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 personnel emails or private email servers (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.

Email

Critical Data and Personal Identifiable Information

Data classified as Critical such as SSN, banking or credit card information, protected health information, and research data with participant identifiers should not be sent via email.

Exchange Online is only approved for up to Restricted data classification. Before using email to share Restricted data, you should consider services approved for Restricted and Critical data, such as:

- Secure Share
- Microsoft at IU Secure Storage

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

Security Breach

There are several ways that a breach can happen.

Those could include:

- 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 Officer and submit a report in EthicsPoint.

In the Remote Work Setting remember:

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

Phishing

Phishing is the fraudulent practice of sending out emails or other messages purporting to be from a reputable company in order to induce individuals to reveal sensitive information.

Many phishing attacks may request personal information by impersonating a leader/manager or other internal staff function (like payroll or HR). If you receive a suspicious message, take the following steps:

1. Recognize - Verify the sender is who you think it is.
2. Rethink - If you can't verify the send, do not click at all!
3. Report - Suspect it's a phish? Send the alert

For more details about how to execute these steps, go to: https://phishing.iu.edu/index.html.

Report Phishing

- Use the Outlook Report Message add-in.
- Forward suspected phishing emails with full headers to phishing@iu.edu.

See the IU Information Security website for more information about phishing education and training.

Regenstrief Institute
www.regenstrief.org

Acceptable Use of IT Systems

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.

Regenstrief Institute
www.regenstrief.org