Critical Data Guide

A guide to handling critical information at Indiana University

Access the guide online at:
go.iu.edu/4MWU

What is Institutional Data?

At IU, institutional information (also called institutional data) applies to data that:

- Is IU's legal responsibility to manage.
- Is substantive and relevant to one or more major administrative functions, or multiple organizational units, of IU.
- Is included in an official university report.
- Is collected as part of the research efforts of faculty, staff, and students.

See policy DM-01: Management of Institutional Data (*go.iu.edu/8qnT*) for more information about institutional data.

There are four classification levels of institutional data at IU:

- **Critical**
- **Restricted**
- **University Internal**
- **Public**

The following chart shows examples of how some data is classified within each data domain. For a complete list, see the Data Classification Matrix: *go.iu.edu/8qyv*

Domain	Critical	Restricted	University-Internal	Public
Cross-domain identifiers (PII)	Full SSN Finger and voice prints Facial scans	Last 4 digits of SSN Residency Date of birth	University ID numbers	Username Full name
Student	Driver's license Passport Financial aid FAFSA Loan applications (GLBA)	Individual grades Academic transcript Student housing Advising notes	Home Address Phone Number	Major Degree
Human Resources	I-9 Form data Payroll direct deposit account number	Home Address	Employee offer letters Faculty tenure recommendations	Salary or compensation Business Address Education & training background
Health	Medical records	Faculty/Staff Immunization record Student administrative health data		
Facilities		Detailed floor plans showing gas, water, sprinkler shut-offs, hazardous materials	Basic floor plans showing egress routes and shelter areas	Campus map showing buildings, names, addresses, parking, lighted pathways, emergency phones, etc.
Finance	Credit card or banking information Invoice number Records related to electronic payments to the university	Tax deductions or contributions Commitments	Capital asset data Chart of accounts Budget Ledger Transactions	

What is Critical Data?

Critical data refers to the most sensitive type of data that demands special care and handling. Mishandling critical data could lead to criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, and/or unauthorized access to this type of information by an individual or many individuals.

For specific examples of critical data for each data domain, see the Data Sharing and Handling Tool (*go.iu.edu/4MWV*).

Critical Personally Identifiable Information

Personally identifiable information (PII) is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information. Some PII is not sensitive, such as full name and email. Other elements can be considered more sensitive, which could result in substantial harm to an individual, including:

- **Identification Numbers:** SSN, driver's license, passport, etc.
- **Financial information:** Bank account numbers, credit & debit card numbers, student loan or billing information.
- **Government-Issued IDs:** Driver's license numbers, State ID card numbers, Passports, and International Visas.
- **Protected Health Information (PHI):** medical records, billing information, and any other details that could identify a patient. Learn more in the section about Critical Health Data.
- **Location Information:** for research purposes, etc.
- **Account credentials:** Passwords, passphrases, PINs, security codes, and access codes.
- **Biometric Identifiers:** Fingerprints, Face ID, eye scans, etc.
- **Other:** information that is linked or linkable to an individual such as medical, educational, financial, and employment information

Given the potential for misuse and harm to the individual in the event of unauthorized access, it is important to store PII in approved locations and limit the collection to what is required.

Critical Student Data

The Family Educational Rights and Privacy Act (FERPA) generally prohibits the disclosure of student education records once a student starts attending a university. Student data protected by FERPA already requires extra precautions, however the most sensitive types of data are classified as critical:

- **Financial Information:** Bank account numbers, credit & debit card numbers, federal student aid (FAFSA), parent tax information, loan or billing information.
- **Student Health:** Individually identifiable health information used for treating students, records maintained by IU student health centers and student counseling programs.
- **Sensitive Identifiers:** Biometrics, driver's license, passports, visa, SSN.

For more information, see *ferpa.iu.edu* or contact the student data steward at *datastu@iu.edu*.

Critical Employee Data

Like students, it is crucial to protect the information that belongs to the staff, faculty, and all employees at IU. Data collected as part of the employment process can be highly sensitive and may be protected by Indiana State data protection laws:

- **Health Data (not covered by HIPAA):** Job-protected leave (FMLA), Worker's comp, disability/ADA claims.
- **Human Relations:** Case files, termination letters.
  Eligibility and Verification Records: I-9 forms and supporting documentation (copy of passport, driver's license, visa), personal profile form.
- **Sensitive Identifiers:** See PII section above.

For more information about staff data, contact the staff data steward at *lkress@iu.edu*.

For more information about faculty data, contact the faculty data steward at *aknshah@iu.edu*.

Critical Health Data

The Health Insurance Portability and Accountability Act (HIPAA) imposes strict privacy and security requirements on individually identifiable health information. Health records and payment details related to healthcare services that are managed by a covered entity fall under Protected Health Information (PHI) (*go.iu.edu/8r2s*):

- **Identifiable Dates:** Date of birth, service time, appointment times, time of death.
- **Identification Numbers:** Account, license plate, SSN, insurance ID.
- **Unique Physical Features:** Biometrics, tattoos, achievements (i.e., world's tallest person).
- **Demographics Attached to Health Data:** Name, home address, contact information, photos.
- **Medical Records:** Tests & diagnoses, treatments, surgeries.
- **Other Records:** Drug and Alcohol Abuse, Sexually Transmitted Diseases (e.g. HIV), and Mental Health Status.

The vast majority of IU units should maintain no PHI whatsoever. For more HIPAA information, see *go.iu.edu/4uj8* or contact the health data steward at *hipaa@iu.edu*.

Critical Financial Data

Examples of services or activities that IU may offer which result in the creation of customer information covered under the Gramm-Leach-Bliley Act (GLBA) could include but are not limited to:

- **Financial Aid:** Federal aid (FAFSA), borrower demographic data, tax returns.
- **Payroll:** Direct deposit, banking information, SSN.
- **Bank Balancing:** Bank transaction history and statements, general ledger activity.
- **Employee, Student, and Vendor Information:** Data collected for governmental taxation requirements (e.g. - Federal, State, Local withholding and tax treaty benefits for payments to a foreign student, employee, or vendor. Other electronic payments made to IU.

For more PCI DSS information, see: *go.iu.edu/4uja*

Critical Research Data

In addition to data regulated by FERPA and HIPAA, other common examples of protected research data include participant PII or PHI. There are special considerations to consider in addition to personal or health data. SecureMyResearch (*securemyresearch.iu.edu*) provides self-service resources and one-on-one consulting to help IU researchers, faculty, and staff meet cybersecurity and compliance requirements for processing, storing, and sharing regulated and unregulated research data.

For more information, see *researchdata.iu.edu* or email the research data steward at *hcoates@iu.edu*.

Employee Responsibilities

As an employee of IU, it is your responsibility to protect the data that you encounter every day. There are several ways that you can take personal responsibility for protecting data at IU. Even if you think you do not have any critical information under your control, there are tools to help make sure. For more information, see: *go.iu.edu/15HR*.

You may also check with the IU Data Management team at *iudata@iu.edu* if you are unsure whether you need to apply special care and handling to the information elements and assets you use.

Storing

When requesting or collecting critical information from individuals or institutional sources, consider these guidelines:

- **Pause and Reflect:** Consider why you need this information, whether it is required for this situation, and if your business purpose be fulfilled without it. If IU maintains the same information elsewhere, access and view the information from the existing source instead of creating another copy.
- **Use it or Lose It:** Keep information, in any form, only as long as it is required for business needs. If unnecessary, securely dispose of the information. If you receive information from another source, also ask the source to avoid sharing unnecessary information with you in the future.
- **Less is More:** If possible, make the information less sensitive while still fulfilling your business needs. For example:
    - Collect only the last four digits of SSNs instead of the complete number.
    - Use university ID numbers instead of more sensitive numbers like SSNs when possible and appropriate.
    - Before creating reports, remove columns containing critical and other individually identifiable data.

For electronic records:
IU's top data storage recommendation is Microsoft at IU Secure Storage (*go.iu.edu/8r2q*). To ensure correct storage security and permissions, employees must request shared storage through the Institutional Storage Request Form (*go.iu.edu/8qoo*). You **MUST** go through this form if you are **storing restricted or critical data classification.** The form will guide you through those considerations and requirements.

- The Data Sharing and Handling Tool (*go.iu.edu/4MWV*) provides guidance on data classification and where to properly store electronic records.
- The Knowledge Base also contains a list of dedicated file storage services that are suitable for storing various types of data: *go.iu.edu/8r2p*.
- For information on encrypting stored critical information, see:
    - About data encryption: go.iu.edu/8r2o
    - Verify that your computer's whole-disk encryption is enabled: *go.iu.edu/8r2n*

For paper records:
- Lock in file cabinets or secure storage rooms.
- If stored in shared locations (like University Archives), ensure that others cannot access your documents.
- **Note:** The IU Warehouse is no longer approved for storing university-internal, restricted, or critical institutional data.

Sharing

Transferring files between computers or people is common, and it's crucial to use appropriate methods for the data being transferred.

Sharing Electronically:
- Secure Share (*go.iu.edu/8r2m*) encrypts data in transit and at rest. It requires IU Login authentication for those affiliated with the university, and requires passwords for non-IU collaborators. Microsoft at IU Secure Storage (*go.iu.edu/8r2q*) can be used to transfer files containing all data classifications.
- Office Message Encryption (*go.iu.edu/8r2l*) encrypts emails containing critical data when it leaves the IU network.
- The SSH (Secure Shell) (*go.iu.edu/8rky*) provides an encrypted channel to transfer data safely. This technique requires password or asymmetric key authentication.
- For information on encrypting transmitted critical data, see:
    - Use SFTP to transfer files (*go.iu.edu/8r2k*)
    - Use SCP to securely transfer files between two Unix computers (*go.iu.edu/8rkA*)

Sharing via Websites:

- Websites must transmit critical information over a secure channel. Generally, secure websites protect the confidentiality of web transactions using Transport Layer Security (TLS) (*go.iu.edu/8r2j*).
- Employees who maintain servers and websites at IU can use the QualysGuard vulnerability scanners to discover vulnerabilities (*go.iu.edu/8r2h*). Periodically scanning and reviewing scan reports is required by IU policy IT-12: Security of Information Technology Resources (*go.iu.edu/4uj7*).

Sharing by Hand:

- Hand over files in person or use trusted couriers. See the Media Disposal Guide for a list of approved couriers: *go.iu.edu/8h6E.* Use locked containers or tamper-evident packaging to protect information from unauthorized disclosure during transit.
- Always require a recipient's signature and follow up to ensure the information made it to the intended recipient.
- Keep your shipping documentation, including the tracking number.

Disposing

All critical information assets must be disposed of securely. Secure disposal means deleting information from media in a way that ensures the data is not recoverable. Never discard or leave any critical information in an area accessible to the public.

Wiping Electronic Storage

Most methods of deleting a file from a computer's hard drive only remove pointers to the actual file — they do not remove the information itself. Most system utilities, and even ways to re-format the hard drive, do not remove the information either.

If you are still actively using the hard drive and are deleting small amounts of critical information (such as a column of SSNs in an old spreadsheet), it is fine to use normal deletion methods and then delete your deleted items.

However, if you are disposing of a hard drive or any storage media, IU policy (*go.iu.edu/4ujF*) requires wiping or destroying them prior to disposal or transfer outside the university. Many utilities will securely wipe a disk or other storage media prior to disposal. Check with your computing support professional about preferred tools, or read about how to securely wipe disk drives: *go.iu.edu/8r2g*.

Hard Drive Destruction

Destroying the hard drive/storage media is often the most effective way to dispose of critical data. There is a university Surplus Data Destruction Service for IU Bloomington (*go.iu.edu/4ujH*) and IU Indianapolis (*go.iu.edu/4ujI*).

For more information about secure data removal, see: *go.iu.edu/8r2e*

Document Shredding:

- IU Bloomington: Shredding & Storage Unlimited
  - Email: Chrisy Gornall (*chrisy@shreddingunlimited.com*)
  - Website: *https://www.midwestdocumentshredding.com/*
- IU Indianapolis: GRM Document Management
  - Email: Customer service (*indorders@grmdocument.com*)
  - Website: *https://www.grmdocumentmanagement.com/company/domestic-locations/*

Disclosing

Directly disclosing or providing critical information elements to an entity outside IU — verbally, on paper, or electronically — is a disclosure. Sharing or disclosure of critical information is sometimes necessary, or even required by law, to complete a business transaction. Through IU policy DM-02: Disclosing Institutional Information to Third Parties, (*go.iu.edu/4ujM*) two processes have been designed to provide the necessary resources for departments to select solutions that meet their needs while minimizing threats to IU data: the Software and Services Selection Process (SSSP) (*go.iu.edu/8r2d*) and Third-Party Assessment (3PA) (*go.iu.edu/8r2c*).

Software and Services Selection Process (SSSP)

The SSSP is used for requesting information technology software, storage, or applications intended for creating, processing, storing, securing, or exchange of electronic data.

The types of products/services that require submission of the SSSP request form include:

- Software and services that interact with Protected Health Information.
- Software and services that collect Payment Card Industry revenue data.
- All products that will interface or be integrated with Enterprise Systems applications.
- All information technology that interacts with Critical or Restricted data, regardless of data domain.
- All new software and services not listed on the SSSP Conditional Allow list (go.iu.edu/8qyy).
- Renewal of existing information technology software and services contracts for which the use case of the product/service has changed from the prior contract term.

Third Party Assessments

In cases involving disclosure of IU institutional data classified as Critical or Restricted data, IU personnel may be redirected to obtain Data Steward (*go.iu.edu/4uj4*) approval to move forward with the procurement process. Data Stewards typically conduct a 3PA before making the decision to grant approval. The 3PA process has six steps:

- Requester submits the 3PA request form with support of the local UITS staff.
- Data Stewards preview the 3PA request form.
- Requester obtains Higher Education Community Vendor Assessment Tool (HECVAT) or other security documentation from the vendor.
- The UISO conducts a targeted information risk assessment and report, if necessary.
- Data Steward records their decision and all parties are notified.
- Acknowledgment and acceptance of Data Steward decision.

For more information about the 3PA process, please see the Knowledge Base (*go.iu.edu/8r2c*).

Other Authorized Disclosures

- In many instances, particularly when a SSN is included, you need to obtain an individual's express written consent for sharing or disclosure. Documents should expressly indicate that their SSN is being disclosed.
- Requests/demands from law enforcement, or from the public under the Indiana Access to Public Records Act (*https://iga.in.gov/laws/2024/ic/titles/5#5-14-3*), should be forwarded to the Office of the Vice President and General Counsel (*vpgc.iu.edu*) **immediately**.

Reporting possible exposures

An unauthorized disclosure of sensitive personal identifiable information is considered a data exposure. Examples include when:

- A computer storing information is compromised or stolen. Information is made available online or via an external application.
- Paper records with the information are disposed in an unsecure manner.
- Computer media is disposed in an unsecure manner.

If at any time you think there is risk of a data exposure without authorization, immediately report an emergency IT incident by outlining the incident details in an email to *it-incident@iu.edu*.

After reporting, immediately follow up by calling the units below in order – no matter what time of day or night (or weekday, weekend, or holiday) – until you reach someone:

- University Information Security Office (UISO) directly at 812-855-8476 (9-5 ET, M-F).
- UITS Network Operations Center at 812-855-3699 (24x7).
- UITS Support Center at 812-855-6789 (24x7)

If outside of work hours, ask Network Operations Center or Support Center staff to contact UITS Data Center Operations so that a PAGE can be sent to the UISO. A representative will then call you back.

If the incident involves a possibly compromised computer, do not use the system. This means you should not do a network scan of the system, run antivirus software, patch the system, reboot, unplug any cables, or power off the system. Taking these actions will destroy important forensic data. Instead, wait for instructions after reporting to the UISO.

Collaborate Safely in Online Meetings

Microsoft Teams (*go.iu.edu/8r2b*) has the ability to distribute research team working sessions, interview participants for clinical research, provide telehealth services, and otherwise collaborate on projects that involve protected health information (PHI).

Precautions

Before hosting a meeting involving PHI on Microsoft Teams, you must consider the following:

- Request a secure team via the Institutional storage request form option to ensure that all meetings in that Team meet the additional security requirements for hosting meetings with PHI at IU.
- Schedule each meeting in the secure Team to have the appropriate safeguards for PHI-related data. For immediate meetings, select the dropdown option to Meet
- Now inside the secure Team channel.
  Store meeting recordings containing PHI within your secure Microsoft Teams channels.

Other Considerations

- Participants can be members of multiple secure Teams and create multiple meetings inside each of these secure Teams.
- Breakout rooms are available in a secure Team; you can enable them in your Microsoft Teams settings and use them normally.
- It is important to keep in mind that any member of a secure Team has the ability to host meetings that may contain PHI. Naming your Team for personal use vs. naming it for use by an entire department likely facilitates a different naming convention for each.

Generative Artificial Intelligence

Generative Artificial Intelligence (GenAI) is a technology that generates new text, images, or other media in response to prompts. While it offers many benefits, it also poses risks, especially regarding data misuse. Sharing information with AI services that lack a data agreement specifying usage and protection measures is like posting it on a public website.

Microsoft Copilot (*go.iu.edu/8r2a*) is covered under the existing contract between IU and Microsoft, and does not save the chat data to train its underlying models. Copilot is approved to interact with data classified up to and including University-Internal if you are logged into Bing with your IU account.

Acceptable uses of generative AI tools can be found on the Knowledge Base: *go.iu.edu/8r29*.

Generative AI Product Request Form

IU has introduced the Generative AI Product Request form to collect usage information for GenAI products and services for use with public and non-institutional data: *go.iu.edu/8qyx*.

This form should be completed after you have submitted the Software and Services Selection Process (SSSP) form for this product. This information will be shared with Purchasing if the product purchase meets the requirements to move forward without additional review by the Chief Privacy Office. In addition, the responses will be shared with UITS, Learning Technologies, and the relevant AI committees evaluating IU's use of Generative AI products.

If a UISO security review is needed during a Third-Party Assessment, vendors must complete an AI Risk Questionnaire, based on industry guidelines. This is in addition to the HECVAT that must be completed during security reviews.

More about AI at IU

University Information Technology Services offers more about AI at IU here: *uits.iu.edu/ai.*