Duke | OFFICE of AUDIT, RISK & COMPLIANCE

Safeguarding Personally Identifiable Information

Personally Identifiable Information (PII) is any information about an individual kept by an organization, including data that can be used to distinguish or trace that person's identity. Some PII is not sensitive, such as what can be found in a phone book, student directory or on a business card; this data is classified as "public" data under Duke's Data Classification Standard. Other PII is sensitive or restricted (see Data Classification Standard), which means that if it is lost, compromised or disclosed without authorization, it could result in harm both to the individual and to the company involved. Harm to an individual could mean identity theft, blackmail, embarrassment, or inconvenience. Harm to the institution includes loss of public trust and reputation, legal liability and/or remediation costs.

Since the dawn of the digital age, security breaches involving PII have contributed to the loss of millions of records. Examples of recent large-scale breaches include Marriott Hotels and First American Financial Corporation, with over 1.3 billion individual records affected. By law everyone at Duke is required to protect privacy and to properly collect, access, use, share and dispose of the PII in our control or under the control of a third party, such as a contractor.

Some examples of PII include:

- First and last name (this is context based)
- Personal identification number, such as Social Security/taxpayer identification number, passport number, driver's license number, financial account number or credit card number
- Address information (street address, email address)
- Telephone numbers (cell, home, business)
- Personal characteristics (facial photos, x-rays, fingerprints, and biometric data such as a retinal scan or voice signature)
- Information that is or can be linked to the above (date/place of birth, race, religion, activities, employment information, medical information, education information, financial information)

Privacy Laws

In the U.S. there is no single, overarching privacy law. Instead, privacy is regulated through many state and federal laws. For example, the Health Insurance Portability and Accountability Act (HIPAA) protects individually identifiable health data, the Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records, Payment Card Industry (PCI) standards help ensure the security of credit card transactions, and the North Carolina ID Theft Protect Act of 2005 requires businesses, charities and government to notify North Carolina individuals if a security breach has compromised any personal information and placed them at risk of identity theft.

In May 2018, the General Data Protection Regulation (GDPR) became effective across much of Europe. The Regulation is designed to ensure the protection of personal data of European Area/European Economic Area (EA/EEA) data subjects. GDPR requires a legal basis for processing and transferring of the personal data of data subjects. GDPR also requires organizations to respond to certain requests from data subjects and to provide notice of breaches of personal information. In addition to the US and EU, many countries have enacted laws regulating actions including the collection, storage, transmission and use of personally identifiable information.

At Duke: Our Responsibility for Protecting PII

- **Physical Security:** Physically secure PII in a locked drawer when not in use or otherwise under the control of a person with a "need to know." Never leave PII unattended on a desk, printer, fax machine or copier.
- **Vendor Security Program Review:** Before engaging a vendor to process PII on behalf of the University, Duke's Information Technology Security Office (ITSO) should conduct a review of the vendor's data protection and security programs.
- **Laptop Security:** Use a privacy screen when in an unsecured area. Lock your computer when you leave your desk and do not leave your laptop unsecured in a public location or vehicle.
- **Consent for Use of PII:** If a data subject provided consent for their PII to be processed, that subject's PII is to be used only for that specific purpose to which they gave consent; no further purposes unless required by law.
- **Protection of PII:** Avoid discussing PII in person or over the phone when you are within hearing distance of anyone who does not need to know the information (including in an airport, in a taxicab, or in a cubicle).
- **Encryption:** Make sure all laptops, USB flash drives and external hard drives are encrypted. Encryption protects the data on the device from being accessed by an unauthorized user if the device is lost or stolen.
- **Transfer of PII:** Don't transfer files or forward emails containing PII to your home computer, personal email account or third parties. Transfers of PII to authorized recipients are to be encrypted.
- **No Sharing of PII:** Do not post PII on the intranet (internal), shared drives, multi-access calendars or on the Internet (including social networking sites) that can be accessed by anyone without a "need to know."
- **Phishing Alert:** Be alert for phone calls or emails (a/k/a phishing) from individuals you do not know attempting to obtain personal or non-public information from or about you.
- **Password Protection:** Never share computer logins or passwords with anyone. Do not permit your computer to remember passwords.
- **Redaction of PII:** When possible, customize or recreate reports or lists to redact sensitive information that is not required for the immediate use of the project.
- **Retention of PII:** Securely dispose of data containing PII in accordance with legal, regulatory and business operational retention disposition requirements. Retain the information no longer than is necessary, and according to Duke's retention guidelines (University Records Retention Guidelines or DUHS Retention, Preservation and Destruction of Records.

You must report all suspected or confirmed privacy incidents to your supervisor or the compliance officer immediately. Do not further compromise the information by forwarding it when reporting an incident.

Please contact Duke Privacy (privacy@duke.edu) with any questions.

Question & Answer

Recently I discovered extensive files on former students who have not matriculated at Duke for over 10 years. Should something be done with these files?

While it appears that this data may no longer be necessary or relevant, there may be a business purpose for the files to be kept. Check with your supervisor to determine the safe and proper disposition of the data according to our records retention policy.

I'm leaving my position to work in another department and my laptop will be transferred to my replacement. What steps should I take to make sure the data is cleared?

Ask the IT help desk to wipe sensitive PII from your drives according to Duke data security standards. Your access to systems that contain PII should be removed unless there is a continuing need for you to access the sensitive PII in your new position.

I plan to work from home while recovering from surgery and need to have access to sensitive employee data during that time. What do I need to be aware of?

Plan ahead; make sure the needed documents can be accessed safely from home. Use a Duke-approved, portable computer that is encrypted, and utilize VPN. Do not transfer or download data to your personal computer or personal email account, or to any non-encrypted device.

I heard my coworker just got a raise and I have access to SAP. Is it okay for me to look up the amount of her raise?

No. Employees should only access confidential information pertaining to other employees for a legitimate business purpose e.g. processing payroll or updating information in the system.