Data Security FAQ

Author: IT Security Office (ITSO)
Version 1.0

Authority
Duke University Chief Information Officer
Duke University Chief Information Security Officer

Purpose
Information is one of Duke’s most valuable assets. The goal of Duke’s data security policy is to allow users to identify, understand, better manage, and employ an appropriate level of security for Duke data.

Why have a policy? To protect sensitive data at Duke, a policy is necessary to outline the requirements for classifying data, who should have access to Duke data, proper data disposal, and data stewardship.

The policy applies to Duke-managed systems and computers as well as to personally owned devices used to access sensitive Duke data. The policy applies to all data for which Duke is responsible, including data located on Duke systems or on your computer or mobile device, in your email account, or stored with a cloud service such as Box.

You are responsible for:
- Accessing only that information and data which you are authorized to access
- Protecting the data
- Knowing the appropriate places to store the data
- Reporting a breach or compromise of sensitive data

Types of data at Duke

Duke's data classification standard requires data owners to assign a level of protection to Duke data - Sensitive, Restricted, or Public.

Sensitive data is the most restrictive data classification category and is reserved for data that Duke is either required by law to protect, or which Duke protects to mitigate institutional risk. Examples: Social Security numbers, credit card numbers, protected health information, student (FERPA) data such as grades.
**Restricted** is the default data classification category. Duke may have a proprietary obligation to protect Restricted data, but disclosure would not significantly harm the institution. *Examples:* payroll information, library transactions.

**Public** is the classification for data that can be accessed by the general public. This includes information that has been approved for publication, such as a press release or information published on [www.duke.edu](http://www.duke.edu). (This does not include information that has been disclosed accidentally.) Access includes Duke University affiliates and general public. *Examples:* public-facing websites, campus maps, and some directory information.

**Extra protections**
Several types of Sensitive data require additional protections, including:
- Student data protected by FERPA (such as grades)
- HIPAA/ePHI data
- Social Security numbers
- Credit card data

Should you have to work with any of them, please contact your IT support or the security offices ([security@duke.edu](mailto:security@duke.edu)) for guidelines on protections for the data.

### Definition of terms

| **Data steward** | The individual(s) ultimately responsible for determining the sensitivity of the data, who can access it, and how it should be protected. Examples: Duke’s Registrar is the data steward for FERPA (student) data such as grades; a principal investigator is the data steward for his/her research project. |
| **Data manager** | Typically an IT administrator responsible for securing the data according to the directives of the data steward. Data managers should have a good working knowledge of how to securely manage systems and applications. |
| **Data users** | The individuals who have been approved by the data steward to access the data. They are responsible for their access to the data, including the security of the account and any data they may have access to or be in possession of. |
| **Researcher** | Research data may go through all classifications during the cycle of research. While a study is in progress, the data may be classified as Sensitive, but after the study is closed and the data shared according to NIH or NSF guidelines, it may be Public. Research budgets are always Sensitive, but federally funded research proposals are often Public (as they may be requested from the funding agency with a FOIA request). |
| **Principal Investigator (PI)** | The PI is considered the data steward for the data in his or her portfolio. |
| **Faculty** | As a teacher, faculty are responsible for following FERPA regulations. In general, this is accomplished by following |
the instructions from the Provost about grading and course conduct.

**Student**
Students involved in research are to follow the research protocols and security requirements and processes. Students involved with Duke Medicine must follow the HIPAA regulations and treat PHI as Sensitive.

**Duke Medicine workforce**
Employees, volunteers, trainees and other persons whose conduct, in the performance of work for a covered entity (e.g., Duke Health System, Private Diagnostic Clinic, School of Medicine), is under the control of such entity, whether or not they are paid by the covered entity.
HIPAA treats all PHI as sensitive.
FERPA applies to Duke trainee interactions.

**IT staff**
IT staff are not usually Data Stewards, so their responsibilities follow the Data Steward's designation and requirements.
IT security policies and procedures are generally considered Restricted.

**Employee**
Expected to follow work instructions and staff policies. Applying common sense to unknown situations and asking for guidance can go a long way to a compliant atmosphere. Responsible for the individual security of their Duke account and the data to which they have been granted access.

Questions about privacy?
The three privacy offices for Duke are:
- Duke Office of Audit, Risk and Compliance: [https://sites.duke.edu/oarc/](https://sites.duke.edu/oarc/)
- DUHS Compliance Office: [https://www.hr.duke.edu/policies/expectations/compliance/duhs_compliance.php](https://www.hr.duke.edu/policies/expectations/compliance/duhs_compliance.php)
- Private Diagnostic Clinic (PDC): [https://pdc.dukemedicine.org/](https://pdc.dukemedicine.org/)

Questions about data stewardship?
Duke University data stewards include:
- Duke Registrar (FERPA data)
- Human Resources (employee data)
- Duke Finance (financial data)
- Duke E-Commerce (credit card data)
- Duke Executive Vice President (Social Security numbers & DukeCard data)
- Researcher/PI is the steward for their protocol/research data

Duke Medicine data stewards can be identified through the Information Asset Management Committee. For other questions about data stewardship or storing/protecting Sensitive data, contact your IT support or the IT security offices ([security@duke.edu](mailto:security@duke.edu)).
Specific questions

Sharing data with collaborators?
Duke offers the Box service (box.duke.edu) for temporary storing and sharing of Sensitive data. In rare instances where mobile storage (e.g., USB flash drive) is needed rather than Box, Sensitive or Restricted data must be encrypted before being placed on the drive.

Storing Sensitive data and Social Security numbers?
A list of approved services to use for storage of sensitive data is available online:
https://security.duke.edu/sites/default/files/Services_Data_Matrix_2015_0.pdf

Only the Executive Vice President can approve storage of SSNs. The security offices (security@duke.edu) can facilitate requests for approval.

- Campus policy: http://security.duke.edu/duke-policy-ssn-usage.
- DUHS policy:
  http://security.duke.edu/sites/default/files/documents/DUHS%20SSNs%202011.pdf
- In Duke Medicine, requests to store SSNs can be made in the eGRC:
  https://egrc.duhs.duke.edu/

Encryption for Sensitive data
For laptop encryption, visit: http://security.duke.edu/whole-disk-encryption
For USB drives and other external devices: Sensitive Electronic Information must be protected on storage devices with whole device encryption or with encrypted files.

Exposure of data
Duke has clear rules around expectations of confidentiality and corrective actions that may result in the exposure of Sensitive or Restricted data:
https://www.hr.duke.edu/forms/confidentiality.php

A data breach could result in a negative impact to Duke’s reputation, or result in fines, loss of a grant or contract, and other financial penalties. In addition, Duke will bear the brunt of notifying and providing fraud monitoring to affected individuals should such a breach occur.

Specific fines and requirements are outlined in the various laws and regulations Duke must adhere to, including:
- PCI – fines for exposure of credit card data or noncompliance
- HIPAA – fines for exposure of patient or clinical data
- NC Identity Theft and Protection Act – Reporting to the NC Attorney General

Report a security incident
If a device has been stolen, first report to local law enforcement or the Duke Police (if the device was stolen at Duke). If a device was lost, contact your local IT support and the security offices (security@duke.edu).

If you are experiencing difficulties with your data or system and suspect a security incident, contact your local IT support and the security offices (security@duke.edu).
Disposal of systems with Sensitive data
All electronic storage should be securely wiped before being disposed of or repurposed. Duke Procurement has an established process to securely dispose of equipment: