Data Security Compliance

Table of Contents

Introduction

Storage of University data on computers and its transfer across networks makes it easier to use and expands functionality. However it is also essential that all University data be protected. It is important to know what kind of data is protected and what security measures the data requires. This webpage describes the University's protected data, provides examples to help classify the data and the retention schedule for the data. It is critical that each individual accept responsibility for safeguarding the confidentiality, integrity, and accuracy of data as (dictated or required) by state and federal law, and University policies and procedures. Although the HIPAA Security Awareness Training Module was developed specifically for HIPAA Protected Data, the information provided is appropriate for protecting ALL types of University data.

Examples of Protected Data

Health Insurance Portability and Accountability Act (HIPAA)

Protected Health Information

In response to growing concerns about keeping health information private, Congress passed the Health Information Portability and Accountability Act of 1996. HIPAA requires agencies that maintain medical records to protect privacy and create standards for the transfer of health data. Agencies are required to follow certain rules to protect the privacy of medical records. Employees are not allowed to access health information unless they need the information to perform their jobs. The only accepted uses of health information are for treatment purposes, payment purposes, or for use for health care operations (e.g. quality assessment, licensing and credentialing, etc.). Any other disclosure of health information must be done with the patient’s written consent. It is required that employees receive training on how to protect health information, whether that information is spoken, on paper, or on a computer.

Examples

- Patient names
- Street address, city, county, zip code
- Dates (except year) related to an individual
- Telephone/fax numbers
- Email, URLs, and IP addresses
- Social Security Numbers
- Account/medical record numbers
- Health and beneficiary numbers
- Certificate/license numbers
- Vehicle IDs and serial numbers
- Device IDs and serial numbers
- Biometric identifiers
- Full face images
- Any other unique identifying number, characteristic, or code
- Payment guarantor's information

Retention

While it is recommended that all medical records be kept forever, HIPAA does not impose a retention requirement. In circumstances where permanent retention is impractical, it is recommended that all medical records be retained for a minimum of 10 years after the last date of treatment, or 10 years after the patient reaches age of majority, whichever occurs later. When records are destroyed, it should be done in a manner that maintains confidentiality.

Family Educational Rights and Privacy Act (FERPA)

Student Records

In order to protect the privacy of student educational records and to allow students and parents greater access to education records, The Family Education Rights and Privacy Act was enacted in 1974. FERPA accomplishes this by requiring that schools keep education records confidential by preventing disclosure to third parties, and by requiring that schools have a policy in place for allowing access to parents and to students over the age of 18. For clarification purposes, educational records are defined as "those records, files, documents, or other materials which contain information directly related to a student, and are maintained by an educational agency or institution or by a person acting for such agency or institution". In addition to educational records, FERPA forbids disclosure of "personally identifiable information", such as a student's social security number, or any other information that may reveal a student's identity.

Examples

- Grades
- Bursar information
- Credit card numbers
- Bank account numbers
- Wire transfer information
- Payment history
- Financial aid and grant information
- Student tuition bills

Retention

- **Student records:** permanent: Includes official academic records (including grades, course evaluations, competency assessments, etc.), change of grade forms, credit by examination forms, faculty grade reports, transcript requests (other than student requested). It is recommended to retain these records permanently, but the legal retention requirement is while active plus 6 years. Actual length of retention is at the discretion of individual departments as long as minimum requirements are met. Destruction of records should be done in a manner that maintains confidentiality.

- **Student records**: non permanent: Records of students who matriculated, whether or not they earned a degree. Includes applications for admission/readmission, letters of recommendation, entrance examinations and placement test reports, advanced placement records, transcripts, transfer credit evaluations, etc. Also includes student placement and continuing education. The legal retention requirement for these records is while active plus a minimum of one year. Actual length of retention is at the discretion of individual departments as long as minimum

requirements are met. Destruction of records should be done in a manner that maintains confidentiality.

- **Student records**: FERPA documentation: Records specific to FERPA, including requests for formal hearings, requests and disclosures of personally identifiable information, student statements on content of records regarding hearing panel decisions, students' written consent for records disclosure, waivers of rights of access, written decisions of hearing panels, etc. Retain while active plus 3 years. Actual length of retention is at the discretion of individual departments as long as minimum requirements are met. Destruction of records should be done in a manner that maintains confidentiality.
- **Data/documents on applicants who do not matriculate**: Records related to applicants who do not matriculate, whether denied admission or accepted and do not enter. Includes applications for admissions/ readmissions, acceptance letters and other correspondence, letters of recommendation, entrance examinations and placement test reports, etc. Retain 1 year. Actual length of retention is at the discretion of individual departments as long as minimum requirements are met. Destruction of records should be done in a manner that maintains confidentiality.
- **Student Loans**: Records related to student loans, including application, approvals, disbursements, repayment, etc. Retain while active plus 6 years. Actual length of retention is at the discretion of individual departments as long as minimum requirements are met. Destruction of records should be done in a manner that maintains confidentiality.

Other Data

The following data are protected by other legislation (PCI, GLBA, Ohio HB 104, Identity) Any combination is protected. (For example: name and credit card number) and in all instances Social Security Numbers are protected.

Advancement Information

- Name
- Graduation class and degree(s)
- Credit card numbers
- Bank account numbers
- Social Security Numbers
- Amount / what donated
- Telephone/fax numbers
- Email, URLs
- Employment information
- Family information (spouse(s) / children / grandchildren)
- Medical history

Research Information

- Funding / sponsorship information
- Human subject information
- Lab animal care information

Employee Information

- Social Security Number (including partials)
- Salary and payroll information
- Name
- Date of Birth
- Home address or personal contact information
- Benefits information
- Performance reviews
- Worker's compensation or disability claims

Business Data (Gramm, Leach, Bliley Act - GLBA)

The Gramm-Leach-Bliley Act of 1999 relates to the protection of personal financial information held by financial institutions. The GLB Act broadly defines “financial institution” as any institution engaged in financial activities on behalf of consumers, and since higher education institutions engage in student loan processing, they are considered financial institutions under the Act. Protected information, however, goes beyond financial aid records. It includes all varieties of personal financial information collected by the university on faculty, students, staff, and others. Examples of protected financial information include financial aid records, credit card and personal check information, salary information and tax records. University offices that maintain protected financial information are required to identify themselves to the Information Security Officer at Computing and Telecommunications Services.

Examples

- Credit card numbers with/without expiration dates
- Bank account information
- Purchasing card numbers
- Social Security or other taxpayer ID numbers
- Contract information (between WSU and third parties)

Retention

GLB does not impose a specific retention requirement for protected financial records, as retentions vary depending on type of record. For specific retention requirements, refer to departmental records retention schedules or the University General Schedule. Some examples are listed below.

- **Accounts Receivable:** Records related to amounts due on open accounts for goods and services provided. Retain while active plus 4 years.
- **Accounting Journals/ Ledgers:** Records used to transfer charges between accounts and for summarizing all transactions. Retain while active plus 4 years.
- **Donor files:** Includes information on major donors, donor giving history, copies of checks, and correspondence. Retain indefinitely.
- **Financial Aid Records:** Files on financial aid recipients. Maintain while active plus 6 years.
- **GLB Documentation:** Records that demonstrate compliance efforts of the institution and its individual units. Maintain for 2 years and until audited.

- **Personnel Files:** Employment records of part time and full time employees. May contain applications, copies of driver's licenses, social security numbers, birth certificate, payroll and salary info, annual contracts, PERS forms, etc. Retain while active plus 6 years. Long term information maintained by Human Resources.

Management Data

- Detailed monthly expenditures statements
- Detailed annual budget information
- Faculty annual conflict of interest disclosures
- University's investment information
- Evaluations

Classifications of Data

Use the following criteria to determine which data classification is appropriate for a particular information or infrastructure system.

Classification of Data	Protected Data (Highest, Most Protected)	Protected Data (Moderate Level of Protection)	Protected Data (Low Level of Protection
Legal Requirements	Protection of data is required by law. See listing below	WSU has contractual obligation to protect the data	Protection of the data is at the discretion of the owner or custodian
Reputation Risk	High	Medium	Low
Other Institutional Risks	Information which provides access to resources, physical or virtual	Smaller subsets of protected data from a school or department	General university information
Access	Only those individuals designated with approved access and signed non-disclosure agreements	WSU employees and non-employees who have a business need to know	WSU affiliates and general public with a need to know
Examples	Medical, Students, Prospective Students, Personnel, Employee, Donor or Prospect, Physical Plant Detail, Credit Card Numbers, Certain Management Information. See more detailed listing below.	Information resources with access to restricted data, Research detail or results that are not restricted data, Library transactions (catalog, circulation, acquisitions), Financial transactions which do not include restricted data (telephone billing), Information covered by non-disclosure agreements, Very limited subsets of restricted data.	Campus maps, personal directory (contact information), Email

Legal Data Checklist

Type of Data	Privacy Statement	Notification Upon Breach	Legislative Private Right of Action	Government Enforcement	Statutory Damages
Ohio HB 104 Personally Identifiable	O	X	O	X	X
FERPA Education Record	X	O	O	X	O
HIPAA Medical Record	X	O	X	X	X
Financial GLBA Banking Record	X	O	O	X	X

X – Application to Data Type

O – Non-application to Data Type

Guidelines

- **Protected Data Technical Regulations** - https://www.wright.edu/information-technology/policies/data-protection-considerations
- **Desktop Protected Data Protection Guidelines** - https://www.wright.edu/information-technology/security/do-it-wright/computing-habits
- **Data Encryption: How Do I Protect Sensitive Information?** - https://www.wright.edu/information-technology/security/encryption#tab=guidelines