

Extended List of Category-I Data

Table of Contents

1. Purpose.....	1
2. Patient Medical/Health Information (HIPAA).....	1
3. Student Records (FERPA).....	2
4. Donor/Alumni Information (BPM, Texas Identity Theft Enforcement and Protection Act, HIPAA).....	2
5. Research Information (Granting Agency Agreements, Other IRB Governance)	3
6. Employee Information (UT System Policy, Texas Identity Theft Enforcement and Protection Act)	3
7. Business/Vendor Data (Gramm-Leach-Bliley Act, Non-Disclosure agreement).....	4
8. Other Institutional Data (Gramm-Leach-Bliley Act, Other Considerations)	4
9. Revision History	4
10. Approvals.....	5

1. Purpose

This document provides an expanded list of representative examples of data classified as Category-I data. This list is provided to help IT- [owners](#) and [custodians](#) with a way to evaluate the level of protections required for their systems.

NOTE: Social Security numbers may be stored on only authorized systems, such as the payroll system. They are released only as required by law; for example, to the IRS for tax purposes.

This list is not all-inclusive, and it does not cover the *release* of information.

2. Patient Medical/Health Information (HIPAA)

The following information is confidential:

- Social Security number
- Patient names, street address, city, county, zip code, telephone / fax numbers
- Dates (except year) related to an individual, account / medical record numbers, health plan beneficiary numbers
- Personal vehicle information
- Certificate / license numbers, device IDs and serial numbers, e-mail, URLs, IP addresses

Document Title

Document Version: Draft/Community Input/Endorsed/Approved

- Access device numbers (ISO number, building access code, etc.)
- Biometric identifiers and full face images
- Any other unique identifying number, characteristic, or code
- Payment Guarantor's information

For more information, see the University of Texas at Austin's [HIPAA](#) Web page.

3. Student Records (FERPA)

The following information is confidential. This applies to both enrolled and prospective student data.

- Social Security number
- Grades (including test scores, assignments, and class grades)
- Student financials, credit cards, bank accounts, wire transfers, payment history, financial aid/grants, student bills
- Access device numbers (ISO number, building access code, etc.)
- Biometric identifiers
- Date of birth

Note that for enrolled students, the following data may ordinarily be revealed by the university without student consent unless the student designates otherwise:

- Name, directory address and phone number, mailing address, secondary mailing or permanent address, residence assignment and room or apartment number, campus office address (for graduate students)
- Place of birth
- Electronic mail address
- Specific semesters of registration at UT Austin; UT Austin degree(s) awarded and date(s); major(s), minor(s), and field(s); university degree honors
- Institution attended immediately prior to UT Austin
- ID card photographs for course instructor use

For more information, see the University of Texas at Austin's [FERPA](#) Web page.

4. Donor/Alumni Information (BPM, Texas Identity Theft Enforcement and Protection Act, HIPAA)

The following information is confidential:

- Social Security number
- Name
- Personal financial information
- Family information
- Medical information

- Credit card numbers, bank account numbers, amount / what donated
- Telephone / fax numbers, e-mail, URLs

5. Research Information (Granting Agency Agreements, Other IRB Governance)

The following information is confidential:

- Human subject information. Refer to the Institutional Review Board Web site (<http://www.utexas.edu/research/rsc/humansubjects>) for more information on research involving human subjects.
- Sensitive digital research data
- Export Controlled Information – ITAR and EAR - Information or technology controlled under the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR) as described below, is confidential:
- Information which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of a controlled item or product. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation.
- Classified information relating to defense articles and defense services;
- Information covered by an invention secrecy order;
- Software directly related to a controlled item;
- This does not include information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges and universities or information in the public domain. It also does not include basic marketing information on function or purpose or general system descriptions of an article or product.

6. Employee Information (UT System Policy, Texas Identity Theft Enforcement and Protection Act)

There can be confusion over which rules apply when an employee is also a student. The rule of thumb is that the student rules apply when the employee is in a [student job title](#).

The following employee information is confidential:

- Social Security number
- Date of Birth
- Personal financial information, including non-UT income level and sources
- Insurance benefit information
- Access device numbers (ISO number, building access code, etc.)
- Biometric identifiers
- Family information, home address, and home phone number **may be revealed unless restricted by the employee**. UT Austin employees can restrict this information in [UT Direct](#).

Document Title

Document Version: Draft/Community Input/Endorsed/Approved

Please note that information considered public, such as employee names, salary, and performance review information, would be released under an open records request.

7. Business/Vendor Data (Gramm-Leach-Bliley Act, Non-Disclosure agreement)

The following information is confidential:

- Vendor social security number
- Credit card information
- Contract information (between UT Austin and a third party)
- Access device numbers (ISO number, building access code, etc.)
- Biometric identifiers
- Certificate / license numbers, device IDs and serial numbers, e-mail, URLs, IP addresses

8. Other Institutional Data (Gramm-Leach-Bliley Act, Other Considerations)

The following information is confidential:

- Information pertaining to the Office of Institutional Relations and Legal Affairs
- Financial records
- Contracts
- Physical plant detail
- Credit card numbers
- Certain management information
- Critical infrastructure detail
- User account passwords
- User Identification Number (UIN)

9. Revision History

Version	Date	New	Original
File Name	<i>[Date of new version]</i>	<i>[Text of change or reason for new version (e.g., submission to review group)]</i>	<i>[Include original text if this is a revision to an Approved version]</i>

Version	Date	New	Original
Extended List of Category-I Data	7/20/11	Converted web page to PDF	
Extended List of Category-I Data	12/7/11	Added additional information under “The following information is confidential:” in Section 5	
Extended List of Category-I Data	2/6/12	Changes made to accommodate inclusion of date of birth as Category I information, per: http://www.supreme.courts.state.tx.us/historical/2010/dec/080172.htm	

10. Approvals

Name	Role	Members	Date
<i>[List committee or subcommittee name]</i> Committee or Subcommittee Name	<i>[Select one and remove the rest]</i> Authoring Input Endorsement Approval	<i>[List members of the committee if a standing body]</i> List members and affiliation.	Date