Extended List of Confidential Data[1]

Please note that this is not an all-inclusive list.

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
- 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

Student Records (FERPA)

The following information is private or confidential. This applies to both enrolled and prospective student data. Education records are records directly related to a student that are maintained by or on behalf of the University.

- Social security number
- Grades (including test scores, assignments, and GPA, class grades and schedules)
- Student financials, credit cards, bank accounts, wire transfers, payment history, financial aid/grants, scholarships, student bills
- Disciplinary Records
- Parent information
- Access device numbers (UTEP 80XXXXXX/88XXXXXX/60XXXXXXXX number, building access code, etc.)
- Biometric identifiers (one or more characteristics like fingerprint, voice print, retina or iris image, DNA, handwriting, facial characteristics, etc.)

Education records do not include:

- Records of instructional, administrative, and educational personnel that are in the sole possession of the maker (i.e. file notes of conversations); are used only as a personal memory aid; not intended to be accessible or revealed to any individual except, in the case of an instructor, a temporary substitute;
- Law enforcement records of the University campus police;
- Medical records and mental health records, including counseling records created, maintained, and used only in connection with provision of medical treatment or mental health treatment or counseling to the student, that are not disclosed to anyone other than the treatment facility;
- Employment records unrelated to the Student's status as a Student; or
- Alumni records;

[1] Adapted from the "*Extended List of Confidential Data*" (http://security.utexas.edu/policies/extended-cat-1), with permission from ITS, The University of Texas at Austin, Austin, Texas 78710-1110

Directory Information means information in a student's educational record that would not generally be considered harmful or an invasion of privacy if disclosed. Note that for enrolled students, the following data may ordinarily be revealed by the university without student consent **unless** the student designates otherwise with the exception of date/place of birth for a student that is also a student employee:

- Name
- Local and permanent address
- Electronic mail address
- Telephone number
- Place of Birth (unless student is also a student employee)
- Field of study; dates of attendance
- Enrollment status
- Student classification (e.g., freshman, first year law school student)
- Degrees awarded
- Certificates and awards (including scholarships) received
- Photographs (e.g., ID card photo for university classroom use)
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Most recent previous educational agency or institution attended

Student Personally Identifiable Information (PII)

Under current regulations, PII includes a student's name AND other direct personal identifiers, such as the student's SSN or student number. PII also includes indirect identifiers, such as the name of the student's parent or other family members; the student's or family's address, and personal characteristics or other information that would make the student's identity easily traceable. The final regulations add biometric records (i.e., one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual, including fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting) to the list of PII and other indirect identifiers, such as date and place of birth and mother's mainden name, as examples of identifiers that should be considered in determining whether information is personally identifiable.

For more information, please visit:

- UTEP's Office of the Registrar (FERPA) Website; or
- UTEP's Handbook of Operating Procedures, Section II: Student Affairs, Educational Records, Chapter 6 (updated February 6, 2015)
- FERPA Final Rule 34 CFR Part 99, Section-by-Section Analysis December 2008

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
- Electronic mail address
- URLs

Research Information (Granting Agency Agreements, Other Institutional Review Board –IRB - Governance)

The following information is confidential:

- Funding / sponsorship information
- Human subject information
- Sensitive digital research data
- Export Controlled Information – International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) as noted 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 or an article or product.

Employee Information (UTS-165, 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 and place of birth
- Personal financial information, including non-UT income level and sources
- Insurance benefit information
- Access device numbers (UTEP ID number, building access code, etc.)
- Biometric identifiers
- Family information, home address, and home phone number ***may be revealed unless restricted by the employee***.

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

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 UTEP 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

Other Institutional Data (Gramm-Leach-Bliley Act, Other Considerations, PCI DSS)

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

Revision History

First Draft: February 6, 2008
Revised: August 17, 2009
Revised: May 19, 2010
Revised: February 17, 2012
Revised: January 28, 2013
Revised: March 14, 2017
Revised: May 9, 2017

Approved: May 9, 2017
Gerard D. Cochrane Jr., Chief Information Security Officer