UW-Madison Sensitive Information Definition

In addition to the information identified below, there are times when a data field is not considered sensitive when used alone but may be so when paired with other data. An example is date of birth. Date of birth is not considered sensitive when it stands alone but if it is available along with social security number and name it is considered sensitive.

Sensitive information may be subject to disclosure under certain circumstances. The University appropriately seeks to maintain systems that protect sensitive information in order to meet a variety of goals.

The data types listed below are those identified as of 6/22/2010

Sensitive Information means:

(i) Institutional Data that could, by itself or in combination with other such Data, be used for identity theft, fraud, or other crimes, including but not limited to,

Restricted Data:[i]

- Social security numbers
- Driver's license numbers and state resident/personal identification numbers
- Financial account number (including credit/debit card) or any security code, access code or password that would permit access to an individual's financial account
- Deoxyribonucleic acid profile, as defined in WI S. 939.74(2d)(a)
- Unique biometric data, including fingerprint, voice print, retina or iris image or any other unique physical representation
- Protected health information (any information about the health status, provision of health care, or payment for health care) (except workman's comp)

Other Data Types:

- Passport numbers and alien registration numbers
- Employee and student identification numbers
- Health insurance identification numbers provided by insurance carriers
- Military ID number
- Personal information such as date of birth and mother's maiden name
- Digitized signatures (ink signatures that have been digitized)
- Garnishments, tax levies, wage assignments
- Beneficiaries, retirement account allocations and investments

(ii) Institutional Data whose public disclosure is restricted by law, contract, University policy, professional code, or practice within the applicable unit, discipline, or profession, including but not limited to:

Data Types:

- Student educational records (including official photos)
- Information in a person's medical record
- Human subjects research information, if the subjects have been promised anonymity
- Trade secrets or other proprietary business information owned by a third party and provided to the University upon a promise of confidentiality for the conduct of research, testing, or training, or in connection with a potential investment or transfer of technology by the University
- Proprietary computer applications or source code to which the University holds a license that restricts further or public distribution
- Exam questions and answers/scoring keys until distributed by the professor
- Bids and proposals until they are opened or the deadline for their submission has passed
- Employment data such as retirement account allocations and investments and designations of beneficiaries
- Employee home address where an employee has asked it not be released
- Documentation of grievance, arbitration, and disciplinary proceedings
- Information about pending research misconduct proceedings
- Financial aid applications and related tax and financial information

- Information and records protected by the attorney-client privilege
- Law enforcement investigation records
- Information disclosed under the University's conflict of interest policies
- Information from a consumer report
- Information derived from servicing or collecting loans from, or accounts payable to, the University
- Data related to those sensitive knowledge, technologies, equipment, software, biological agents or related services that are subject to United States Government export controls

(iii) University and personal security measures, including but not limited to,

Data Types:

- Passwords for access to University facilities or computer systems
- Security codes and combinations for locks
- Key codes
- Security plans
- Security procedures
- Threat assessments and preparedness strategies
- Law enforcement deployment plans
- Operational instructions for law enforcement officers and other emergency personnel

and (iv) Institutional Data whose value would be lost or reduced by disclosure in advance of the time prescribed for its authorized public release, or whose disclosure would otherwise adversely affect the University financially, including but not limited to,

Data Types:

- Research data or results prior to publication or the filing of a patent application
- Non-patentable technical information or know-how that enhances the value of a patented invention or that has independent commercial value
- Information relating to the University's intention to buy, sell, or lease property whose disclosure could increase the cost of that property for the University or decrease what the University realizes from that property (like real property appraisals)
- Computer applications to which the University owns the code

Please direct questions about this document to policy@cio.wisc.edu.[ii]

SensitiveInfo		Issued by:	Office of the CIO	Published at:	http://www.cio.wisc.edu/policies/
Effective:	Jan 8, 2009	Review in:	two years	Maintained by:	Office of the CIO, Policy and Planning
Revised:	Jun 22, 2010 (Rev A)	See:	https://wiki.doit.wisc.edu/confluence/display/POLICY/SensitiveInfo/		

[i] Restricted Data includes Personal Identifying Information (PII) as specified in Wisconsin's data Breach Notification Law (statute Section 134.98), plus Protected Health Information (PHI) as defined under the Health Insurance Portability and Accountability Act (HIPAA). Sensitive Information includes Restricted Data, but Restricted Data receives additional protection. More information on Restricted Data can be found at http://www.cio.wisc.edu/security/initiatives/restricted.aspx.

[ii] The definitions in this document are directly derived from work done at the Michigan State University. Our thanks to them for allowing us to use their work.