COMPUTING SERVICES
Section: 135-3 APPENDIX A
Effective: 01/17/2012
Supersedes: 04/15/2010
Review Date: TBD
Issuance Date: 01/17/2012
Issuing Office: Administrative Computing & Telecommunications (ACT)

APPENDIX A – DEFINITIONS

1. SENSITIVE ACTIVITIES

For the purposes of this document, Sensitive Activities are defined as anything that involves the storage, entry, processing, transmission, or viewing of Sensitive Data.

2. SENSITIVE DATA

Sensitive Data is any data that is regulated by law or limited by contractual agreements between the University and other business partners.

3. CRITICAL VULNERABILITIES

A Critical Vulnerability is one where an exploit or proof-of-concept code is publicly available or being actively exploited.

4. FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

FERPA covers all student data. We may disclose without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance as long as we honor the students disclosure preferences from Tritonlink. If any data is present that has been flagged for non-disclosure or the disclosure option is not checked and enforced then the data is considered sensitive.

5. GRAMM-LEACH-BLILEY ACT (GLBA ACT)

The GLB Act, officially known as The Financial Modernization Act of 1999 includes privacy provisions to protect consumer information held by financial institutions. Because of the student loan activity, the University is considered a financial institution under the GLB Act. Family Educational Rights and Privacy Act (FERPA) compliance places the University in compliance with FTC privacy rules under the GLB Act.

6. CALIFORNIA PUBLIC RECORDS ACT CODE 6250-6270

The Act mandates public access to records held by the University. The Act also provides exclusions for access to certain types of records or data. Examples of data that are excluded include personal payroll/employee data such as state and federal tax withholding. The Act requires that we protect the privacy and integrity of this data and its use at the University.

7. CALIFORNIA STATE SENATE BILL SB 1386

SB 1386 became operative in 2003. It "requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system, following discovery or notification of the security breach, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

The bill defines “personal information” as follows:

An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

1. Social security number.

2. Driver's license number or California Identification Card number.

3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

8. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

HIPAA is a federal law establishing national standards that provide for the privacy and security of an individual's health information. Information created or received by a health care provider or health plan that includes health information or health care payment information plus information that personally identifies the individual patient or plan member.

Personal identifiers include: a patient's name and email, web site and home addresses; identifying numbers (including Social Security, medical records, insurance numbers, biomedical devices, vehicle identifiers and license numbers); full facial photos and other biometric identifiers; and dates (such as birth date, dates of admission and discharge, death).

9. PAYMENT CARD INDUSTRY (PCI) STANDARDS

The PCI standard is a contractual agreement between the University and our merchant bank. The agreement covers our handling of credit card numbers, magnetic stripe contents, CVC numbers, and expiration dates. In addition to the standards outlined above for sensitive systems, PCI requires additional security and has its own set of standards that must be met.

10. CALIFORNIA STATE ASSEMBLY BILL (AB) 1950

Enacted in 2004, AB 1950 requires any business that is the data custodian of personal information about a California resident to “implement and maintain reasonable security procedures and practices” to protect the data. Personal information disclosed “pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information.”

11. CALIFORNIA STATE ASSEMBLY BILL (AB) 1298

Enacted in 2007, AB 1298 expands the definition of “personal information” as defined in SB 1386 to include health information and medical record information.

12. HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH (HITECH) ACT

HITECH is part of the American Recovery and Reinvestment Act of 2009. It includes provisions for breach notifications by entities covered by HIPAA that disclose unsecured protected health information (PHI). The Act states that notifications “shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved.”

HITECH requires covered entities to notify affected individuals, the Secretary of HHS, and in some cases the media. The Secretary must post on the HHS web site the names of covered entities for breaches that involve more than 500 individuals.