University of California
San Francisco

UCSF Policy 650-16 Addendum F, Data Classification Standard

Policy Type	**Document Owner**	**Department Contact**
Standard	Patrick Phelan	UCSF IT Security
Issue Date	**Effective Date**	**Reviewed/Revised Date**
4/24/17	4/24/17	8/9/19

Purpose

The purpose of this Data Classification Standard is to direct the method for classifying UCSF's electronic data. This document demonstrates UCSF's determination of the Protection Levels of each classification of UCSF data in compliance with University of California Policy BFB-IS-3: Electronic Information Security.

Overview and Scope

This standard applies to all electronic data managed and owned by UCSF, wherever it may be stored. Data storage locations may include, but are not limited to, data centers, data accessed by or stored remotely on electronic devices, and UCSF data that is stored with contracted third parties including Business Associates, cloud service providers, vendors, contractors, and temporary staff.

This data classification methodology in no way supersedes any state or federal government classifications assigned contractually or otherwise.

UCSF electronic data shall be classified according to the Data Classification Model described in this standard. The Data Classification Model will be used to determine the appropriate data classification for UCSF electronic data created, maintained, processed, or transmitted utilizing electronic resources. Under this model data will be classified in accordance with external regulatory, internal policy and other contractual requirements, and in accordance with the potential adverse impact of loss, theft, or unavailability of the data.

In the event a specific set of electronic data is classified as fitting within a combination of two (2) or more of the data classifications, that data shall be managed in accordance with the most restrictive and/or highest applicable data classification.

University of California
San Francisco

In the event a specific set of electronic data *does not* fit into the current Data Classification Model, please contact UCSF IT Security for the determination of the appropriate data classification. UCSF's Data Classification Standard serves as a location-specific interpretation of UC system-wide policy and, therefore, supersedes many of the requirements of the UC Institutional Information and IT Resource Classification Standard, although the system-wide standard may be referenced for guidance on the classification of data types not documented within this location-specific model.

UCSF IT Governance shall review the Data Classification Standard at least annually and update as needed to include additional data types and reflect any changes to protection level classification or policy and legal requirements.

Business Impact

Considerations for evaluating the potential adverse business impact to UCSF due to loss or compromise of the electronic data's confidentiality or integrity include:

- Loss of critical UCSF operations
- Negative financial impact (actual money lost, lost opportunities, value of the data itself)
- Damage to UCSF's reputation
- Potential for regulatory or legal action
- Violation of UCSF's missions, policies, or principles
- Requirement for corrective action or repairs

University of California
San Francisco

Data Classification Model:

	Restricted Data	Sensitive Data	Internal Data	Public Data
UCOP Protection Level	P4 - High	P3 - Moderate	P2 - Low	P1 - Minimal
Policy & Legal Requirements	Protection of data is required by federal or state law or regulation, or contractual obligation, and may be subject to data breach notification requirements. UCSF Minimum Security Standards apply.	Protection of data is required by the data owner or other confidentiality agreement, and may be required by federal or state law or regulation, or by policy. UCSF Minimum Security Standards apply.	Data may not be specifically protected by federal or state law or contractual obligation, but are generally not intended for public use or access. Protection of data is governed by University policy. UCSF Minimum Security Standards apply.	Protection of data is governed by University policy. UCSF Minimum Security Standards apply.
Access	Only authorized individuals with approved access; signed confidentiality, non-disclosure, and/or other applicable agreement as permitted by law; and a *business need to know.*	Only authorized individuals with approved access and a *business need to know.*	Intended audience for data access under the design of the system.	Data intended to be readily obtainable by the public.
Adverse Business Impact Statement	**High Adverse Impact to:** • Regulatory or legal action • Violations of UCOP or UCSF policies and principles • UCSF's reputation • UCSF's finances • UCSF critical operations	**Moderate Adverse Impact to:** • Regulatory or legal action • Violations of UCOP or UCSF policies and principles • UCSF's reputation • UCSF's finances • UCSF critical operations	**Low Adverse Impact**	**Minimal Adverse Impact**

University of California
San Francisco

Data Types	• Personally Identifiable Information (PII) • Protected Health Information (PHI) • Research Health Information (RHI) • Payment Card Industry (PCI) Data • Confidential Security Information • Licensed Proprietary IP and Product Development Information	• University Intellectual Property • De-identified Health Information • Employee Information • Sensitive Faculty Activities • Student Information • Donor Information • Current Litigation/Investigation Materials • Contracts • Physical Building Designs • Financial Information	• Public Directory Information • Routine Business Records and Email • Research Using Publicly Available Data	• Public-facing Websites • Published Research • Maps • Press Releases • Course Catalogs • Parking Regulations

Restricted Data Types:

1. Personally Identifiable Information (PII)

a. PII is protected by federal and state laws and regulations, including federal regulations administered by the U.S. Department of Homeland Security (DHS), and is defined by DHS as "any information that permits the identity of an individual to be directly or indirectly inferred, which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual." PII must be protected prior to release in accordance with the Public Records Act or other disclosures required by law.

b. PII includes but is not limited to the following:

1. Any of the following stand-alone elements:
   i. Full Social Security Number (SSN)
   ii. Driver's license or State ID number
   iii. Passport number

iv. Visa number
v. Alien Registration Number
vi. Fingerprints or other biometric identifiers

2. Full name in combination with any of the following elements:
   i. Mother's maiden name
   ii. Date of birth
   iii. Last 4 digits of SSN
   iv. Citizenship or immigration status
   v. Ethnic or religious affiliation

2. Protected Health Information (PHI)

a. PHI is protected by the federal Health Insurance Portability and Accountability Act (HIPAA) and includes all individually identifiable health information, held or transmitted by a Covered Entity or its business associate, that relates to the health or health care of an individual, and specifically includes but is not limited to the following:
   1. Information about an individual's past, present, or future physical or mental health condition, or provision of and/or payment for healthcare to the individual, which includes at least one of the following identifiers:
      i. Names
      ii. All geographic subdivisions smaller than a state, except for the initial three digits of the zip code if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people
      iii. All elements of dates, except year, and all ages over 89 or elements indicative of such age
      iv. Telephone numbers
      v. Fax numbers
      vi. Email addresses
      vii. Social security numbers
      viii. Medical record numbers
      ix. Health plan beneficiary numbers
      x. Account numbers

xi. Certificate or license numbers
xii. Vehicle identifiers and serial numbers, including license plate numbers
xiii. Device identifiers and serial numbers
xiv. Web Universal Resource Locators (URLs)
xv. Internet Protocol (IP) addresses
xvi. Biometric identifiers, including finger and voice prints
xvii. Full face photographs and any comparable images
xviii. Any other unique, identifying number, characteristic, or code, except as permitted for re- identification in the Privacy Rule. This includes APeX-generated identifiers such as Encounter ID and PatID.

3. Research Health Information

a. Research health information is individually identifiable health information collected outside of the covered entity setting (i.e., the researcher is acting solely as a researcher with no clinical interaction, and the data is collected outside of UCSF's HIPAA covered entity providers). Examples of research health information include: data obtained from subjects during interviews or surveys, and the investigators do not review or alter the subjects' health records or make treatment decisions as part of the research; data obtained from records open to the public or existing research records; and data obtained using tests that do not go into the medical record because they are part of a basic research study and the results will not be disclosed to the subject.

4. Payment Card Industry Data (PCI Data)

a. PCI Data is data subject to the Payment Card Industry Data Security Standard/s (PCI-DSS), developed by the PCI Security Standards Council and adhered to by the University, and includes but is not limited to the following:
   1. Cardholder Data:
      i. Primary Account Number (PAN)
      ii. Cardholder name
      iii. Service code
      iv. Expiration date
   2. Sensitive Authentication Data:
      i. Full magnetic stripe data

ii. CAV2/CVC2/CVV2/CID
iii. PIN/PIN Block

5. Confidential Security Information

a. Information descriptive of the specific security measures that safeguard restricted (confidential or personal) information resources represents a special class of information that should be protected from unauthorized access or disclosure. Such information – whether hardware configurations, management controls or security practices, or procedures employed – could provide a roadmap for malicious individuals to attack University applications, systems, and networks. Confidential security information includes but is not limited to the following:
   1. Documentation of known or potential vulnerabilities and risks
   2. Results of security scans and assessments
   3. Implementation/ configuration details for security devices and tools (e.g. specific software version numbers, network diagrams, vendor definition updates, and software modules)
   4. Implementation/ configuration details for systems that provide security services for restricted data types. Security services include services which ensure confidentiality, integrity, and availability for other systems (e.g. authentication systems, VPN's, systems management consoles, backup systems, credential stores, data loss prevention systems, system inventories, and encryption)
   5. Firewall and intrusion detection system logs
   6. Private credentials used to authenticate users, processes, and systems
   7. Security incident documentation including (e.g. indicators of compromise, remediation plans, remediation efforts, data identification analysis, documentation of malicious presence in the environment, and forensic analysis)
   8. Permission attributes identifying the resources to which an individual has access

6. Licensed Intellectual Property and Product Development Information

a. Licensed intellectual property and product development information is third party confidential information licensed to outside industries to the extent of identifying the products or services the third party (typically pharma and biotech industries) is developing with UCSF, and the third party's commercialization plans for those products and services. Licensed intellectual property and product development information includes but is not limited to the following:

University of California
San Francisco

1. Medical indication for which the third party is developing the product
2. Information identifying the chemical structure of a lead therapeutic candidate in development
3. Financial terms of the license
4. Proprietary company information relating to existing products in the industry partner's pipeline
5. Information relating to the product development timeline

Sensitive Data Types:

1. University Intellectual Property

a. University intellectual property relates to creations of the mind and includes electronic data which the University may patent or gain from financially through intellectual property commercialization partnerships and commercial entities. University intellectual property includes patents, copyrights, trademarks, and trade secrets, but does not include copyrighted materials which are publicly available.

2. De-identified Health Information

a. Health information that does not identify an individual, and for which there is no reasonable basis to believe that the information can be used to identify an individual, is not individually identifiable health information (PHI) and is considered de-identified. The Health Insurance Portability and Accountability Act (HIPAA) allows for two methods of de-identification: Expert Determination and Safe Harbor.

b. Expert Determination requires that a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods applies those principles and methods and determines that the risk is very small that the information could be used to identify an individual who is the subject of the information. Methods and results of the analysis must be documented.

c. For Safe Harbor, all of the following 18 identifiers must be removed:
   1. Names
   2. All geographic subdivisions smaller than a state, except for the initial three digits of the zip code if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people
   3. All elements of dates, except year, and all ages over 89 or elements indicative of such age
   4. Telephone numbers

5. Fax numbers
6. Email addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate or license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) addresses
16. Biometric identifiers, including finger and voice prints
17. Full face photographs and any comparable images
18. Any other unique, identifying number, characteristic, or code, except as permitted for re-identification in the Privacy Rule. This includes APeX-generated identifiers such as Encounter ID and PatID.

d. Options for obtaining validated de-identified data sets include: requesting de-identified data as part of the UCSF Enterprise Data Request Process; utilizing data from UCSF de-identified data applications; or requesting validation of your own de-identified data set through validation services provided by UCSF Enterprise Information and Analytics.

e. Both Safe Harbor and Expert Determination methods, even when properly applied, yield de-identified data that retains some risk of identification. Although the risk may be very small, it is not zero, and the possibility remains that de-identified data could be linked back to the identity of the patient to which it corresponds.

3. Employee Information

a. Employee information is managed by Human Resources or Academic Personnel, protected by state or federal laws and regulations, including regulations of the United States Department of Labor, and is data directly associated with an employee or applicant for employment, which must be protected prior to release in accordance with applicable policy and law. Employee information includes but is not limited to the following:
   1. Contents of Employment applications, other than Personally Identifiable Information (PII)
   2. Personnel files

3. Performance evaluations
4. Benefits information

4. Sensitive Faculty Activities

a. Sensitive faculty activities include information about the teaching, research, and service activities of UCSF faculty. Sensitive faculty activities include, but are not limited to the following:
    1. Academic research or teaching activities involving use of live animal research subjects, or other controversial matters
    2. Academic research or teaching activities involving control of hazardous materials, or technology which presents a high risk of harm to persons or property
    3. Academic service activities involving affiliation with an organization which, if made known to the general public may result in risk of bodily or other harm to the individual

5. Student Information

a. The Family Educational Rights and Privacy Act (FERPA) protects from disclosure most records that are directly related to a student and that are maintained by UCSF or a party acting for UCSF. Student information includes but is not limited to the following:
    1. Grades, exam papers, and test scores
    2. Class lists
    3. Student course schedules
    4. Evaluations and disciplinary records
    5. Student financial records
    6. Directory information for students who have requested that information about them not be released as public information
    7. Employment records of a student, if the student's employment is contingent upon the fact that he or she is a student

6. Donor Information

a. Donor Information is information about financial asset donations that has a stated purpose at the bequest of the donor, and includes but is not limited to:
    1. Donor's full name
    2. Donor contact information
    3. Securities donated

4. Real estate donations
5. Planned giving arrangements
6. Amount/value donated

7. Current Litigation/Investigation Materials

a. Current litigation materials are electronically stored information that pertains to a current litigation hold implemented by UCSF's Office of General Counsel. These materials include but are not limited to:
    1. Word, Excel, PowerPoint, or other office application documents
    2. PDF documents
    3. E-mail
    4. Calendar items
    5. Electronic voice mail
    6. USB drives

8. Contracts

a. Contracts are electronic copies of agreements, to which UCSF is a party, creating obligations enforceable by law. Electronic contracts include but are not limited to the following formats:
    1. Word documents
    2. PDFs
    3. Scanned images

9. Physical Building Designs

a. Physical building designs are defined as detailed floor plans, architectural drawings, or other renderings that show restricted areas, animal care facilities, mechanical spaces, or other spaces in the buildings not considered accessible for public use. Physical building designs include but are not limited to the following formats:
    1. Office documents (Visio, Word, etc.)
    2. AutoCAD
    3. PDFs

University of California
San Francisco

4. Images
5. Videos

10. Financial Information

a. Financial information includes monetary facts about UCSF and/or other parties who participate in financial transactions with UCSF that are used in billing, credit assessment, loan transactions, and other similar activities, that must be protected prior to release in accordance with the California Public Records Act or other disclosures required by law. Financial Information includes but is not limited to:
   1. Taxpayer identification numbers
   2. Credit ratings
   3. Account numbers
   4. Account balances

Internal Data Types:

1. Public Directory Information

a. Public directory information includes information about academic personnel, staff personnel, and students that is designated as public information in accordance with UCOP policy, and includes but is not limited to the following:
   1. Non-Personal Academic Personnel Information:
      i. Name
      ii. Date of hire or separation
      iii. Current position title
      iv. Current rate of pay
      v. Organization unit assignment including office address and telephone number
      vi. Full-time, part-time, or other employment status
   2. Staff Personnel Records Designated as "Public Information"
      i. Name
      ii. Date of hire
      iii. Current position title

iv. Current salary
v. Organizational unit assignment
vi. Date of separation
vii. Office address and office telephone number
viii. Current job description
ix. Full-time or part-time, and appointment type

3. Public Student Directory Information (unless a student notifies UCSF in writing or via electronic procedures that any or all of these may not be disclosed (FERPA block))
   i. Name
   ii. Address (local and/or permanent)
   iii. E-mail address
   iv. Telephone numbers
   v. Date and place of birth
   vi. Field(s) of study
   vii. Dates of attendance
   viii. Grade level
   ix. Enrollment status
   x. Number of course units in which enrolled
   xi. Degrees and honors received
   xii. Most recent previous education institution attended
   xiii. Photo
   xiv. Participation in officially recognized activities, including athletics
   xv. For participants on intercollegiate University athletic teams: name, weight, and height