SDSU HealthLINK Center
Research Data Security Classification and Handling Guide

JANUARY 8, 2026

Information Classification Standard

The SDSU HealthLINK Center has adopted the CSU Information Security Policy and Standards as a minimum information classification standard. These standards outline three levels of classification and standards (Protected Level 1, 2, and 3) to which information must be secured. Along with these standards, the following guidelines and policies have been established by the SDSU HealthLINK Center to assist in reducing exposure to information and data loss.

Information security is essential whether information is conveyed electronically, over the phone, or in written documents, whether it is acquired, transmitted, processed, transferred, and/or maintained by the SDSU HealthLINK Center.

All SDSU HealthLINK Center faculty, staff, project leaders, and entities working on behalf of HealthLINK Center are subject to these guidelines and policies, and to SDSU Information Security policies and procedures, including periodic Security Awareness Orientation training.

Table 1. Protected Level 1 (PL-1) Data / Confidential

Protected Level 1 information is information primarily protected by statutes, regulation, other legal obligations or mandates. The CSU and SDSU have identified standards regarding the disclosure of this type of information to parties outside of SDSU/SDSURF and controls needed to protect the unauthorized access, modification, transmission, storage, or other use. Level 1 Confidential information is intended for use by SDSU/SDSURF and access is limited to those with a "business need- to-know."

Example of Protected Level 1 information (HIPAA-Protected):

- Passwords or credentials
- PINs (Personal Identification Numbers)
- Credit/debit/payment card numbers with any of the following:
    - cardholder name
    - expiration date
    - card verification code
- Social Security number or Tax ID with name

- Driver's license number, state identification card, and other forms of international identification (such as passports, visas, etc.) with name or social security number
- Name with bank account information or bank account information with password, security code, or any other access code information
- Private key (digital certificate)
- Contact phone number (if sensitive or unlisted)
- personal e-mail address (when linked to identifying data)
- Home address
- Health insurance information
- Medical records related to an individual (HIPAA-protected data, including disability information, diagnoses, treatment information, medication history)
- Psychological counseling records related to an individual
- Electronic or digitized signatures
- Employee's Personally Identifiable Information (PII), including:
    - Mother's maiden name
    - Gender identity
    - Birthplace (city, state, country)
    - Birthdate
    - Employee net salary
    - Physical description/personal characteristics
    - Employment history (including recruiting information)
    - Biometric information
    - Electronic or digitized signatures
    - Parents' and other family members' names
- **Other examples of participant data often collected by health researchers (these data are likely to be collected on a screening questionnaire, an enrollment form, or demographics and health questionnaires) include, but are not limited to:**
    - Study ID/Recruitment ID master list linked with participants' full names
    - Caregiver or family member's full name for studies targeting children/youth
    - Sexual orientation
    - Sexual identity
    - Current/past symptoms (e.g., asthma-related symptoms, coughing, dizziness, etc.)
    - Current/past physical or mental health problems (e.g., heart diseases, hypertension, diabetes, asthma, kidney failure, depression, sleep disorder, etc.)
    - Current/past use of medications (e.g., diabetes, heart diseases, GI medications)
    - Current /past use of treatments (e.g., chemotherapy, drug therapy, radiation therapy, blood transfusion, etc.)
    - Ever applied for disability or workers' compensation?
    - Have/had any physical disabilities?
    - Have/had any psychological disorders?
    - Residence ZIP code, when combined with other unique identifiers

Table 2. Protected Level 2 (PL-2) Data / Internal Use

Protected level 2 information must be guarded due to proprietary, ethical, or privacy considerations. University standards will indicate the controls needed to protect unauthorized access, modification, transmission, storage, or other activities.

Example of Protected Level 2 information:

- Student name (FERPA-protected**)** with personally identifiable educational records
    - Courses taken
    - Schedule
    - Test scores
    - Financial aid received
    - Advising records
    - Educational services received
    - Dietary restriction
    - Disciplinary actions
    - Photograph
    - Most recent educational agency or institution attended
    - Participation in officially recognized activities and sports
    - Weight and height of members of the athletic team
    - Grades
    - SDSU identification number (RedID)
    - Age
    - Race & Ethnicity, only if not linked with name or sensitive data, but when linked with health, disability, or participant data→becomes PL-1
    - Gender
    - Transcripts
    - E-mail addresses
- **Employee name with personally identifiable information**
    - Birthdate (full: mm-dd-yyyy or mm-dd)
    - Emergency contact home address
    - Emergency contact personal telephone number
    - Emergency personal contact information (name, cell phone, pager)
    - Personal telephone numbers
    - Personal vehicle information
    - Personal email address
    - Parents' and other family members' names
    - Payment history
    - Preferred language to speak
    - Speak English/Spanish
    - Employee evaluations
    - Background investigations
    - Photograph (voluntary for public display)
- Other
    - Physical (wet) signatures
    - Legal investigations
    - Sealed bids
    - Trade secrets or intellectual property, such as research activities
    - Location of highly sensitive or critical assets (e.g, safes, check stocks, etc.)

    - Library circulation information
    - Vulnerability or incident information
    - Licensed software
    - Attorney/client communications
    - Third-party proprietary information per contractual
- **Other examples of participant data often collected by health researchers (these data are likely to be collected on a screening questionnaire, an enrollment form, or demographics and health questionnaires) include, but are not limited to:**
    - Gender
    - Race/ethnicity
    - Occupation
    - Acculturation status
    - Nativity
    - Employment
    - Education level
    - Marital status
    - Household composition (number of children/adults in the household)
    - Self-rated health
    - Pregnancy
    - Income
    - Days living with the child
    - Name of the school/child care center the child attended
    - Name and Location of the usual primary health care provider

Table 3. Protected Level 3 (PL-3) Data / Generally Regarded as Publicly Available

Protected level 3 is information that is regarded as publicly available. This information is either explicitly defined as public information (such as state employee salary ranges), intended to be available to individuals both on-campus and off-campus (such as employee work email addresses), or not specifically classified elsewhere in the protected information classification standard. Publicly available information may still be subject to review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

Example of Protected Level 3 information:

- Student information designated as Educational Directory Information (excluding grades):
    - Student name
    - Major field of study
    - Dates of attendance
    - Degrees, honors, and awards received
- Employee Information (including student employment)
    - Employee title
    - Employee name (first, middle, last; except when associated with protected information)
    - Enrollment status
    - Department employed
    - Work location and telephone number

- Work e-mail address
- Employee classification
- Status as a student (such as TA, GA, ISA)
- Employee gross salary
- SDSU identification number (RedID)

Classification Guidance

- Where several categories apply, use the highest level of security, that is, use Level 1 versus Level 2 and so on. Questions about the proper classification of a specific piece of information should be addressed to the HealthLINK Systems Administrator.

Non-State (personal) information (both electronic and non-electronic)

- Personal such as personal credit reports, personal bank statements, or even contact information from a synchronized cell phone or PDA, must not **be stored on the SDSU HealthLINK Center systems**, as the SDSU HealthLINK Center does not assume responsibility for securing this information, and many systems may not be secured for this information by default. Personal information does not just pertain to first-party personal information (yours), but also to any third-party personal information (someone else's).

The full information on the Information Classification Standard is available in the CSU and SDSU IT Security Policies, Standards, and Procedures.

Information Labeling Guidelines

- Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Protected Level 1 (PL1)", "Confidential", "Protected Level 2 (PL)", or "Internal Use" may be written or designated in a conspicuous place on or in the information in question.
- Other labels identifying the data classification may be used at the discretion of individual business units or departments.
- If no marking is present, the SDSU HealthLINK Center information is presumed to be "the SDSU HealthLINK Center Confidential" unless expressly determined to be the SDSU HealthLINK Center Public information by an SDSU HealthLINK Center employee with authority to do so.

Information Handling Guidelines

The following guidelines are presented to assist project leaders, project managers, coordinators, employees, and clients working with the SDSU HealthLINK Center in securing information.

Sensitive Data Storage Best Practices

Storing and Sharing Protected Data Guide

Zoom Meetings for HIPAA