California Health Sciences University

UNIVERSITY

CHSU DATA GOVERNANCE POLICY

PURPOSE

CHSU relies on the confidentiality, integrity, availability, security, and privacy of its data and information in order to successfully conduct its operations, meet the expectations of internal and external stakeholders, and provide services. This policy establishes uniform data governance standards and identifies the shared responsibilities for assuring the integrity of CHSU's data and that data is efficiently and effectively managed to serve the needs of the University (CHSU). CHSU values access to timely, accurate, and consistent information while fully appreciating the basic security and privacy requirements involved. Controlled access by employees to administrative information is necessary to support business functions.

This policy also provides direction on the classification, ownership, and retention of CHSU's data and information for CHSU as well as clarifying accountability for data and information.

SCOPE

Scope of Data and Information covered by this policy: This policy applies to all of CHSU's Critical Data and Information (both electronic and non-electronic), including data and information hosted on CHSU's information systems and stored outside of CHSU (e.g., in a cloud service). "Critical Data and Information," in this context, includes email, personal and shared files, specific application system records, website contents, and operating system–level information and any data that connects to CHSU systems.

This policy applies to all CHSU administration, faculty, staff including students employed by the university acting in the capacity as an employee, contractors, users, and external parties at the University who may be creators and/or users of such data. The policy also applies to third parties who access and use CHSU systems and IT equipment or who create, process, or store data owned by CHSU.

The definition of critical data and scope of this policy will be reviewed annually.

POLICY STATEMENT

1. All university data is owned by CHSU and, as such, all administration, faculty, staff, contractors, users and external parties of CHSU are responsible for appropriately respecting and protecting the University's data and information assets.
2. For CHSU to effectively manage and safeguard the data assets, procedures must be in place to guide appropriate data access, ensure the security of the data, and provide a means to address procedural exceptions.
3. Roles, including both those of individuals with data responsibilities like data champions, stewardships, and custodianships and those of eligible users, are necessary to support data integrity and security. See Appendix A
4. Sharing information across organizational boundaries should be facilitated, where appropriate and applicable, in compliance with the data-sharing policy.
5. A centralized data administration function should reinforce a set of definitions for commonly consumed data,
6. Data integration across CHSU is encouraged where appropriate to foster data accuracy and uniformity and to demonstrate an understanding of CHSU's institutional complexity, various data systems, and differing data formats.
7. Data must be safeguarded to maintain the confidentiality and privacy of personally identifiable information consistent with requirements of state and federal laws and regulations. Data should be classified based on an agreed-upon data classification scheme as set forth in CHSU's Data Classification Standards Policy.

8. Access to CHSU data may be limited by legal requirements or restrictions in contract or licensing agreements. Otherwise, access to data will be based on the business needs of the University and the ability of CHSU to achieve its mission. Except where not permitted under data sharing policy guidelines, employees should have access to the data needed to perform their responsibilities, without regard to arbitrary barriers.

9. Before individuals will be allowed to access CHSU data, they must complete training in the use and attributes of the data, functional area data policies, and CHSU policies regarding data. Training will be coordinated by the Data Champion.

10. A terminology/taxonomy shall be developed by the IT (Information Technology) Committee and IAER (Institutional Assessment, Effectiveness, and Research) Office, or an appropriate subset, to provide a framework for requesting and producing consistent data across all levels of the enterprise. The definitions will be accessible to all CHSU data users and included in training.

11. Data, as a CHSU asset, must be safeguarded and managed at all points and across all systems, from creation to archive, through coordinated efforts and shared responsibilities to ensure its accuracy. Each functional area will develop and implement processes for identifying and correcting erroneous or inconsistent data.

12. Extraction, manipulation, and reporting of CHSU data is permitted only in connection with CHSU educational or business purposes:

    - Personal use of CHSU data, including derived data, in any format and at any location, by University employees is prohibited unless approved by President's Executive Council.

    - Where feasible, before any University data or information is used outside the Data Steward's functional unit, the Data Steward should consult with the functional area manager and data champion to verify that their use of the data is appropriate and permitted.

13. Before decisions are made concerning data retention and data archiving, the appropriate Data Champion must be consulted.

14. A centralized data request is a formal request for data made to the IAER. The request must be made consistent with the protocols and procedures set by the IAER. The request must identify the purpose of the request, who will use the data if the request is approved, the specific data needed, and the deadline by which the data is needed. After the request is made, the IAER will review it to verify that the data request is legitimate, that the request is not duplicative of other requests, that the request is in compliance with the University's policies and regulations, and that the requestor has authority to view and use the data. If the IAER determines that the request is appropriate, the IAER will pull the data responsive to the centralized request, prepare it in the requested format, and forward the data to the requestor or the requestor's department, and identify any restrictions on use of the data.

15. Individuals seeking permission to access data who are not approved to do so under the access plan or in their defined roles must submit a written request for nonstandard access to the Chair of the IT Committee. The request must include the access being sought and the reason for the request. The Chair and/or designee will send the request to the appropriate Data Steward for review and decision. The Data Steward will report the decision to the appropriate Data Champion and to the requestor's manager.

    Any exceptions to this policy will be documented and approved by the IT Committee.

Noncompliance

Violations of this policy will be investigated like other allegations of staff or student misconduct at CHSU. CHSU will determine appropriate disciplinary actions and/or sanctions for noncompliance up to and including termination of employment or dismissal from the University. Decisions will be based on the severity and frequency of violation. Additionally, in order to protect its data assets, CHSU may pursue legal action against the violator(s).

California Health Sciences University

Appendix A
Data Governance Roles

Roles and responsibilities	Related Data Asset(s)	Accountabilities and Responsibilities
IT Committee	Enterprise data	• Review and approve the policy on regular basis
President's Executive Council	Enterprise data	• Retain records used in the decision-making process for key decisions to demonstrate best practice and risk assessment • Review and approval of this policy and any updates to it as recommended by the IT Committee • Ensure ongoing compliance with the IT Committee in their respective areas of responsibility • Ensure oversight of data protection issues either through their own work or an IT Committee or other governance arrangement • Ensure the Policy mandate to the entire organization
Data Champion, *Accountable for overall management and integrity of specific datasets or data domains within the organization*	Information of CHSU and its business data assets	• Final approval for protected CHSU information • Final approval for protected CHSU data assets • Final approval for CHSU data classification schemes • Compliance with Data governance policy, processes, and procedures • Ensure the proper usage of data assets within compliance/legal requirements and CHSU internal objectives • Approve user roles/profiles/classes • Review access including application data held in network directory locations • Responsible for review and approval of data classification, data retention, and master data changes • Ensure appropriate availability of information • Promote the use of data as a strategic asset

		• Play a critical sponsorship role in those projects that create or improve data services pertinent to the data for which the data owner is accountable • Provide final decision-making authority for data escalations • Product ownership of data services pertinent to the data for which the data Champion is accountable including but not limited to Mobile Device Management services, reference data management services, and data quality services • Maintain data ownership throughout the data or information lifecycle, from operational system to data lake to analytics • Approve data standards • Approve business models
Data Stewards: *Manage institutional data and access to the data of particular organizational units* *Responsible for defining and enforcing data standards, policies and procedures within area of expertise or domain*	Various specific data assets pertaining to their area of responsibility such as HR, payroll, reporting, etc.	• Where appropriate, authorize access to their data assets as per data governance principles and instructions • Develop documentation, business rules, data standards, and data quality rules for the use and development of their data assets with the assistance of the subject matter experts and the architects • Act as first point of contact for all data governance issues and change control processes for their data assets • Assess impact of any high-risk data governance issues and escalate to relevant Data Owners with supporting recommendations • Assist in creating data standards and data operational procedures • Assist in creating data rules • Assist in creating data classification schemes • Define master data and reference data sets and mappings • Accountable for data glossary and data catalog maintenance and publication and communication of those artifacts • Contribute to the creation of data policy and data standards operating procedures • Be a data literacy champion within CHSU

		• Approve data visualizations containing data for which the Data Steward is responsible
Data Custodians: *Individuals within units with direct control over information systems that house institutional data* *Manages the technical aspects of data storage, access and security, ensuring that data is stored and protected according to established policies.*	Enterprise data maintained by IT teams, e.g. data warehouse	• Maintain and administer technical security and audit trails of the data • Responsible for data availability, capacity, accuracy, and consistency • Oversee and implement data operations and database backup and restore • Responsible for technical standards and policies
Data Protection Officer: *Ensures that data governance practices comply with relevant laws, regulations, and industry standards, and manages risk associated with data management practices.*	Enterprise data	• Lead the data protection compliance and risk management function, with responsibility for advising how to comply with applicable privacy legislation and regulations • Advise on all aspects of data protection and privacy obligations • Monitor and review all aspects of compliance with data protection and privacy obligations • Act as a representative of data subjects in relation to the processing of their personal data • Report directly on data protection risk and compliance to executive management

RESPONSIBILITIES

A. This policy is the responsibility of the Vice President of Operations.

HISTORY (R*)

Approval Date:

08/20/2024

Revision Date(s):

06/26/2024

01/31/24

Reviewed Date(s):

06/26/2024

05/30/2024

RACI

R: VP of Operations

A: VP of Operations, IT Director, Director of Institutional Assessment, Effectiveness, and Research (DIAER)

C: VP of Operations, Director of DIAER, Legal

I: CHSU President's Executive Council, Vice Presidents & Directors