California Health Sciences University

CHSU PRIVACY OF PERSONAL INFORMATION POLICY

I. PURPOSE

The purpose of this policy is to ensure the protection of personal information that is collected, stored, and/or shared by the University.

II. PRIVACY OF PERSONAL INFORMATION

CHSU is responsible for taking all reasonable and appropriate steps for the protection of the confidentiality, availability, privacy, and integrity of information in its custody. This includes the physical security of the equipment where information is processed and maintained, and the preservation of information in case of intentional, accidental, or natural disaster. In addition, CHSU is responsible for the maintenance and currency of applications that use this information.

III. POLICY STATEMENT

Enforcement of CHSU's Information Security Policies and compliance with Federal and State regulations regarding information technology is the responsibility of the President. Policy enforcement may be delegated to the Executive Director of IT. All CHSU Information Security Policies will be reviewed on an annual basis for compliance with applicable Federal and State regulations.

This policy applies to all students, faculty and staff, consultants, or any other persons having access to CHSU Information Technology. All unauthorized modifications, deletions, or disclosures of information included in CHSU data resources that compromise the integrity of CHSU's educational, scholarly, and administrative programs, violate individual privacy rights, or constitute a criminal act are expressly forbidden.

This policy is not limited to those systems and equipment operated and maintained by Information Technology Service department, but applies to all data, systems and equipment on and off campus that contain protected, confidential, or mission critical data, including college and departmental level systems and equipment, and vendor hosted solutions.

IV. APPLICABILITY AND AREAS OF RESPONSIBILITY

1. **Privacy of Personal Information**

    - All users of CHSU information systems or network resources are advised to consider the open nature of information disseminated electronically and must not assume any degree of privacy or restricted access to information they create or store on CHSU systems. No CHSU information system or network resource can absolutely ensure that unauthorized persons will not gain access to information or activities. However, CHSU acknowledges its obligation to respect and protect confidential and protected information about individuals stored on CHSU information systems and network resources.

2. **Collection of Personal Information**

    - To comply with state and federal laws and regulations, CHSU will not collect personally identifiable information unless the need for it has been clearly established.

3. **Where such information is collected:**

    - The University will use reasonable efforts to ensure that personally identifiable information is adequately protected from unauthorized disclosure.

    - The University will store personally identifiable information only when it is appropriate and relevant to the purpose for which it has been collected.

4. **Access to Personal Information**
   Except as noted elsewhere in CHSU policy, information about individuals stored on CHSU information systems may only be accessed by:

    - The individual to whom the stored information applies or his/her designated representative(s).

    - Authorized CHSU employees with a valid related business need to access, modify, or disclose that information.

    - Appropriate legal authorities**.**

   When appropriate, authorized CHSU personnel following established procedures may access, modify, and/or disclose information about individuals stored on University information systems or a user's activities on CHSU information systems or network resources without consent from the individual. For example, CHSU may take such actions for any of the following reasons:

- To comply with applicable laws or regulations.
- To comply with or enforce applicable CHSU policy.
- To ensure the confidentiality, integrity or availability of CHSU information.
- To respond to valid legal requests or demands for access to CHSU information.

If CHSU personnel accesses, modifies, and/or discloses information about an individual and/or his/her activities on CHSU information systems or network resources, staff, faculty, and any other employees will make every reasonable effort to respect information and communications that are privileged or otherwise protected from disclosure by CHSU policy or applicable laws.

5. **Access to Electronic Data Containing Personal Information**

- Individuals who access or store protected data must use due diligence to prevent unauthorized access and disclosure of such assets.
- Browsing, altering, or accessing electronic messages or stored files in another user's account, computer, or storage device is prohibited, even when such accounts or files are not password protected, unless specifically authorized by the user for university related business reasons. This prohibition does not affect:
- Authorized access to shared files and/ or resources based on assigned roles and responsibilities.
- Authorized access by a network administrator, computer support technician, or departmental manager where such access is within the scope of that individual's job duties.
- Access to implicitly publicly accessible resources such as University websites.
- CHSU response to subpoenas or other court orders.

V. THE FOLLOWING INDIVIDUALS AND ORGANIZATIONAL UNITS HAVE POLICY RESPONSIBILITIES:

The President delegates the Information Security responsibility to the Executive Director of IT

VI. UNIVERSITY COLLEGES AND DEPARTMENTS MUST:

1. Adhere to all CHSU Security Policies and have plans and procedures for the protection for their data. These plans and procedures must ensure business continuity, including protection against natural, accidental, or intentional disasters. The plans must include access control, password security, backup and off-site storage of mission critical data, and procedure for cost/effective security systems including virus scanners and firewalls that insure protection against known vulnerabilities.
2. Inform users granted access to personal information of their responsibilities to secure such data from unauthorized release.
3. Develop and maintain control records in a secure environment.
4. Establish monitoring procedures to identify unauthorized access to or anomalous activity.
5. Report suspected unauthorized acquisition of personal information to the Information Security Officer.

VII. DATA END USERS MUST:

1. Protect the resources under their control, such as access passwords, computers, and data they download.
2. Report any unauthorized acquisition or anomalous activity of personal information to the IT Services Department which may have resulted in the release of personal information to unauthorized individuals.

- Policy Owner: Executive Director of Information Technology
- Effective Date: 9/02/2020
- Revised Date:
- Approval by the President: 9/14/2020