The University of Southern California
Office of Culture, Ethics, and Compliance
Data Privacy Compliance Program Document

I. Introduction

The Office of Culture, Ethics and Compliance (OCEC) is responsible for developing a comprehensive **Data Privacy Compliance Program ("Privacy Program")** to facilitate University of Southern California (University) schools, departments, units and other entities that may collect, receive, use, disclose, and store data are compliant with University data privacy policies, procedures, and applicable state, federal, and local statutory and regulatory requirements.

The Privacy Program's focus is to proactively identify and address data privacy risks. The scope, structure, core functions and activities of the Privacy Program are updated as necessary to reflect organizational and policy changes, regulatory and statutory changes, and best practices for addressing data privacy compliance risk.

II. Scope of the Privacy Program

The following statutory and regulatory requirements, standards, and other laws and regulations, along with any others deemed applicable to the University, are within the scope of the Program:

- California Confidentiality of Medical Information Act (CMIA);
- Family Educational Rights and Privacy Act (FERPA);
- Federal Trade Commission's Red Flags Rule (Identity Theft Prevention);
- General Data Protection Regulation (GDPR);
- Gramm-Leach-Bliley Act (GLBA);
- Health Insurance Portability and Accountability Act (HIPAA); and
- Payment Card Industry (PCI) standards.

III. Data Privacy Principles

The University is committed to the appropriate care and custody of personally identifiable data. The following Data Privacy Principles form the core of University's position on collection, use and retention of personally identifiable data and are incorporated in the Privacy Program.

1. Privacy by Design

The University shall design processes and information technology associated with the collection, use, and disclosure of personally identifiable information (PII) in a

manner that focuses on complying with applicable legal and regulatory data protection and privacy requirements and following best practices.

2. Transparency and Notice

The University shall provide reasonable advance notice on the collection, uses, disclosures, retention, and disposal of PII information.

3. Choice

Prior to collecting, using, disclosing, or retaining information about individuals, University, when required to do so, shall provide individuals with the ability to choose whether to and by what means to provide their information.

4. Uses and Disclosures

When using and disclosing PII, whenever possible the University shall take reasonable and appropriate steps, except when permitted under law or regulation, to provide individuals with the minimum amount of PII necessary for the intended purpose, and disclose the minimum amount of PII necessary to individuals who have a need to know the information in order to perform their job responsibilities or contractual obligations.

5. Information Protection

The University demonstrates its commitment to protecting PII by implementing privacy and information security controls and safeguards to address issues related to the confidentiality, integrity, and availability of data.

6. Rights Related to Information

The University shall uphold individuals' rights (i.e. access, amend, delete) related to their information, in accordance with applicable data privacy laws and regulations.

7. Accountability

The University expects its employees and Third Parties with which it has a contractual relationship to adhere to these principles and support the University's commitment to respect the privacy of individuals and their data. The University will investigate alleged violations of its data privacy policies and, as appropriate, take corrective measures.

IV. Elements of an Effective Compliance Program

The University has developed a compliance framework and standards tied to external guidance regarding effective compliance programs, including the United States Sentencing Commission's Federal Sentencing Guidelines. The following are part of the University's framework and are addressed in the Privacy Program:

- Culture, Governance and Compliance Oversight
- Compliance Risk Identification and Assessment
- Policies, Standards and Systems
- Education, Training and Outreach
- Monitoring, Auditing and Program Evaluation
- Investigations, Corrective Action and Enforcement

V. Implementation of the Data Privacy Compliance Program

The University's Data Privacy Compliance Program includes the elements stated above and addresses its organizational structure and data privacy compliance risks. The Privacy Program is founded on both risk-based and proactive core components designed to promote and support a culture of compliance and prevent and detect instances of noncompliance.

1. Culture, Governance, and Compliance Oversight

The **Data Privacy Advisory Compliance Committee (DPAC)** will support the Program by advising the OCEC on plans and initiatives to (1) help USC faculty, staff, and students understand and comply with applicable laws, rules, and policies covering privacy and related issues; (2) prevent and detect violations of law, regulations, and university privacy policies; and (3) periodically assess compliance risks in the area of data privacy and advise on core mitigation strategies in accordance with the DPAC charter, which is reviewed annually.

DPAC membership shall represent the following units/functions and others may be asked to participate on an as needed basis:

- Academic Records and Registrar
- Academic Senate
- Admissions
- Advancement
- Auxiliary Services
- Business Services (Purchasing and Contracts)
- Financial Aid
- Human Resources
- Information Security
- Keck Medicine – Healthcare Compliance
- Office of General Counsel
- Office of Research
- Office of Culture, Ethics, and Compliance

- School of Dentistry
- Staff Assembly
- Strategic and Global Initiatives
- Treasury Services

The **Vice President, Office of Culture, Ethics, and Compliance** provides leadership and direction on USC's compliance programs and initiatives. The Vice President provides periodic updates to the Audit, Compliance, Risk, and Privacy Committee of the USC Board of Trustees on status of USC's compliance programs, which includes Data Privacy.

The **Assistant Vice President, Institutional Compliance, Office of Culture, Ethics, and Compliance** works across USC and with key stakeholder to develop and implement comprehensive compliance area programs such as Data Privacy that meet the elements of effective and efficient programs including, but not limited to training, policies, monitoring, data analytics and reporting.

The **Director of Data Privacy** is accountable for establishing and maintaining the USC data privacy program; reviewing compliance with regulatory, statutory, policy, and procedural requirements related to the collection, use, and disclosures of data. The Director of Data Privacy collaborates with various offices to assist them with their data privacy compliance obligations, and closely interfaces with them on mutual concerns.

Faculty, staff, professional students, and volunteers should meet the professional, ethical and regulatory standards associated with preserving data privacy when performing their individual roles, and to adhere to USC policies, procedures, and the Code of Conduct.

Additional responsibilities related to data privacy may be assigned to persons in **supervisory, management and leadership positions**.

2. Compliance Risk Identification and Assessment

A risk assessment approach is used to identify, prioritize, and address data privacy risks within USC. Action plans are created and responsible owners identified for completing tasks to address the identified risks.

3. Policies, Standards and Systems

The Privacy Program is based on a framework of policies, standards, systems, and procedures that articulate USC's commitment and processes to meet applicable data privacy regulatory and statutory requirements. The Privacy Program is aligned to the USC Compliance and Ethics Program Governance and Standards. This includes the development of core data privacy policies that address compliance requirements as well as supplemental procedures and standards that provide guidance on activities;

assuring compliance with the policies. The DPAC can be consulted to review policies, procedures, and standards including providing input on implementation, dissemination, and adherence.

4. Education, Training and Outreach

An essential component of the Privacy Program is education, training, and outreach to ensure that policies and procedures are disseminated and understood by USC faculty, staff, professional students, and volunteers. The Privacy Program involves periodically evaluating and revising existing training and education in particular risk areas and identifying areas where new or additional training is necessary.

The OCEC partners with key stakeholders to develop and implement a training, education, and outreach/awareness program based on identified risk areas and need. The program may consist of a multi-channel approach for delivering activities – including annual and ad-hoc online and in-person training as well as ongoing education and awareness initiatives through additional techniques (i.e. FAQs, tips, newsletters, meetings).

5. Monitoring, Auditing, and Program Evaluation

Internal monitoring and auditing are expectations of USC's Privacy Program in order to promote compliance with data privacy policies, procedures, and controls. OCEC coordinates with USC's Audit Services to conduct assessments that assist in identifying potential data privacy risk areas.

The Privacy Director performs periodic evaluations of the effectiveness of the Privacy Program and makes appropriate changes, as necessary. The Privacy Director documents lessons learned from the evaluations and adopts revisions aimed at improving and enhancing the Privacy Program and how the University approaches data privacy risk.

6. Investigations, Corrective Action and Enforcement

Faculty, staff and other employees are expected to report data privacy concerns of potential violations or other offenses promptly to their respective supervisors and/or to the OCEC. Actual and potential violations of data privacy policies and procedures will be investigated, and when appropriate corrective and/or disciplinary action taken.

9/17/2020