UCSD Information Security and Privacy Council Charter

**Scope:**
The UCSD Information Data Security and Privacy Council (ISPC) is advisory to the UCSD Chief Ethics and Compliance Officer, who chairs the UCSD Compliance, Audit, Risk, and Ethics Committee (CARE). The ISPC will replace the Information Technology Security Workgroup and assume the duties previously assigned to that Workgroup. In addition, the ISPC will provide guidance on the appropriate application of State and Federal privacy breach notification laws.

**Problem Statement:**
The ISPC is needed to achieve a cohesive organizational structure aligning responsibility, authority, and accountability for effective enterprise computer security and information privacy. Because State and Federal privacy rules are complex, potential privacy and security breaches need to be evaluated promptly to avoid fines and to determine whether the facts about the breach meet the criteria for external notifications to consumers and government agencies.

**Activities:**
1. Design and oversight of adequate monitoring, auditing, and enforcement mechanisms to identify and correct root causes of security weaknesses in high-risk circumstances
2. Communication of information security and privacy policy to campus constituents
3. Oversight of optimal use of appropriate technical solutions (hardware and software) to address technical security issues
4. Coordination of responses to periodic information technology security surveys to provide an accurate campus-wide view of computer security
5. Development of policy and technical solutions to protect the privacy and security of confidential, personally identified information (PII) and protected health information (PHI) in all formats, e.g., paper, electronic, written, oral, transmitted, and/or stored.
6. Review of privacy and security incidents investigated by the Computer Incident Response Team (CIRT) and reported to the ISPC to:
   - Determine whether the incident requires external breach notifications or meets an exception in accordance with State / Federal privacy breach notification laws.
     - Cal SB541: 5-business days for licensed facilities for breach of PII.
     - Cal AB1298: timely notices for breach of unencrypted electronic PII data.
     - Fed HITECH: Notify individuals without delay (within 60-days). For breaches > 500 individuals, also notify OCR, media (if the 500 individuals are in the same state or jurisdiction), web page.
     - Fed HITECH: Annual notice: OCR (within 60 days), document exceptions.
     - Review risk assessment documentation: Analysis for risk of financial and personal harm to individuals in accordance with the HITECH laws.
     - Assure that notification decisions are reached in a fair, consistent, objective, and efficient manner without undue delays and in compliance with State / Federal Privacy Laws concerning breach notifications.
     - Provide guidance on remedial actions and sanctions to assure that fair, consistent procedures are implemented across the campus and clinical enterprise.
     - Document analysis of decisions not to report incidents to individuals and the Office of Civil Rights in accordance with HITECH laws
7. Share collective expertise to evaluate incidents and determine whether to expand the scope of the incident investigation / remediation processes to other areas within UCSD Health Sciences, UCSD campus and UC systemwide.
8. Provide advice to the Campus and Health Sciences’ Privacy Officers / Directors and Information Security Officers on information security and privacy issues pertaining to State / Federal privacy and security laws, including review of proposed standards and guidelines.
9. Periodically report activities / outcomes to the leadership of CARE, campus, and Health sciences executive leadership, and the UC Office of the President’s Privacy Official.
Members

Chair

- Charlotte Klock, Interim Chief Information Security and Privacy Officer, UCSD

Members

- Ed Babakanian – Chief Information Security Officer, Health Sciences; and Medical Center Representative
- Doug Bennett, Scripps Institution of Oceanography Representative
- Stephanie Burke, Resource Management & Planning Representative
- Paul Craig - Chief Human Resources, Safety & Risk Management Officer, UCSD Medical Center
- Emily Deere, Administrative Computing & Telecommunications
- Ron Espiritu, School of Medicine Representative
- Marianne Generales, Research Affairs Representative
- Lee Giddings – Chief Compliance and Privacy Officer, Health Sciences
- Don Larson, External & Business Affairs Representative
- Gabriel Lawrence, Administrative Computing & Telecommunications (consultant)
- Debbie McGraw, Academic Affairs Representative
- Dan Park, UCSD General Counsel
- Ed Spriggs, Student Affairs Representative

Meeting Frequency

The Council will conduct virtual and/or in-person meetings as often as needed to meet its objectives.

Ad Hoc Members

Based on nature and scale (size) of a privacy or security incident and notification requirements, additional ad hoc members may be included. Ad hoc members may serve in an advisory role, consultant role, or will be asked to assist with identifying resources and strategies to enable implementation of efficient incident response procedures, incident remediation, and communications with leadership at the campus and systemwide levels.

Ad hoc members could include representatives from the following areas (non-inclusive list):
- UCSD Registrar and FERPA Coordinator – William Haid
- UCSD Health Sciences Counsel
- Campus and Health Science Communications, for media / large scale notices
- UCSD CIRT representatives, for security incidents
- UCSD Audit Management & Advisory Services
- UC Systemwide Privacy Officer
- UC Systemwide General Counsel

Health Sciences Privacy Board

A separate UCSD Health Sciences Privacy Board has been established which will report to this Council. The Health Sciences Privacy Board will perform similar activities to those outlined in this Charter for the Health Sciences enterprise and will consist of the following members: Chief Compliance/ Privacy Officer, UCSD Health Sciences; Chief Human Resources, Safety & Risk Management Officer, UCSD Medical Center; Chief Information Officer, UCSD Medical Center; General Counsel for UCSD Health Sciences; and Director, Compliance/Privacy Program, UCSD Health Sciences.