Attachment 1

UNIVERSITY OF CALIFORNIA

# Office of Ethics, Compliance and Audit Services

# Compliance Plan 2021-22

# Table of Contents

# I. EXECUTIVE SUMMARY

The Office of Ethics, Compliance and Audit Services (ECAS) presents its annual compliance plan (Plan) for fiscal year (FY) 2021-22. This plan is developed through an extensive, systemwide risk assessment process. The Plan represents input and involvement of many compliance professionals across the University and highlights the focus of our systemwide priorities for FY 2021-22.

## Methodology

ECAS in cooperation with the Campus Ethics and Compliance Officers (CECOs) and the Healthcare Compliance Officers (HCCOs) throughout the system develop annual risk assessments and related compliance plans for their locations and medical centers. These plans are developed through close partnerships with experts within Risk Services, Internal Audit, and UC Legal. During this process, compliance professionals review location metrics and processes; conduct surveys and interviews of campus leadership and key risk owners; review new or pending regulations, guidance, and legal findings; and consult internal and external subject matter experts.

# II. RISK PRIORITIES AND PLANNED RISK ACTIVITIES

The annual risk assessment process and related plans ensure that compliance officers throughout the system are focusing their resources on the highest compliance risks at their location and throughout the system. ECAS evaluates the individual campus plans and develops the overarching Plan for the University.

The systemwide risk priorities and the resulting Plan are described below.

## A. RESEARCH COMPLIANCE

Research compliance aims to address shared research risk priorities through stakeholder facilitation and engagement with our academic community and administration, the development of systemwide communications, the development and implementation of training and education materials, and the use of systemwide risk assessments.

### REGULATORY ENVIRONMENT

The U.S. federal government heavily regulates the basic and applied research conducted at the University of California (UC). Various state laws, U.S. federal government regulations, and UC policy all converge to create a complex regulatory matrix for research compliance. Multiple federal agencies are responsible for regulations governing research, from the Food and Drug Administration's (FDA) compliance oversight of clinical trials to the Drug Enforcement Agency's oversight of controlled substances use in research, and the Department of Health and Human Services oversight and enforcement of Human

Subjects Research Protections. Federal and state privacy laws, such as the Health Information Portability and Accountability Act (HIPAA) and the Confidentiality of Medical Information Act (CMIA), govern research and use of patient health information. Additionally, federal funding agencies, such as the National Science Foundation (NSF) and the National Institutes of Health (NIH), issue policies and guidelines that further shape the research compliance landscape.

## KEY PROJECTS

### Training and Professional Development

ECAS collaborates closely with UC Legal and Research Policy Analysis and Coordination (RPAC) in providing regular guidance and training to campuses. In addition to these ongoing efforts, ECAS will conduct compliance assessments of high-risk research areas throughout the system and provide more formal training offerings throughout the year to ensure systemwide awareness and compliance.

#### *Digital Research Data Security and Privacy*

The use of technology, including artificial intelligence (AI) and machine learning (ML), in the advancement of healthcare, is a rapidly emerging area and depends fundamentally on the use, access, and sharing of large volumes of patient health data. Health data, including protected health information (PHI), is used in the research context to inform these tools, draw conclusions, and inform policy. This transformation creates significant compliance risks throughout the system.

Therefore, ECAS will be developing and hosting a two-day conference on clinical research, privacy, and human subjects testing compliance to address many of these risks. The conference will provide compliance training and updates on high-risk areas to personnel throughout the system, in areas such as:

- Certificates of confidentiality in health records,
- Genomics research,
- Governance for research use of health data,
- Research deemed non-human subject research when HIPAA privacy rules apply,
- De-identification standards in light of emerging technology, and
- Collaborative research and associated intercampus transfers of PHI.

This conference will also facilitate cross-functional, systemwide communication and collaboration and allow ECAS to identify future opportunities for engagement and training.

*Systemwide Training*

In addition to the two-day conference, ECAS will be providing a suite of additional research compliance training in 2021, including:

- Systemwide Ethics & Compliance Briefing for Researchers module: This module, which will launch in the first quarter of FY 2021-22, will address general ethics and compliance matters, foreign influence matters, and other issues related to researchers, such as disclosure of affiliations with foreign entities to federal funding agencies.
- ClinicalTrials.gov training: ClinicalTrials.gov Protocol Registration and Results System (PRS) is a database of privately and publicly funded clinical studies conducted around the world. Federal regulations, enforced by the FDA, require registration and submission of summary results information for all applicable clinical trials into PRS. To help facilitate compliance with these regulations, ECAS, with campus participation, will develop a practitioner's training in this area during FY 2021-22.

*Assessments*

ECAS will perform a series of targeted assessments throughout the system this fiscal year to identify opportunities to strengthen existing policies and processes related to:

- Human subjects protection programs,
- Animal research,
- FDA regulated research,
- Controlled substances,
- Sub-recipient monitoring, and
- Data ownership and security.

Additionally, ECAS will be monitoring compliance with research data security and Cybersecurity Maturity Model Certification (CMMC) requirements.

## Foreign Influence

In accordance with the FY 2019-20 Internal Audit Plan approved by the Board of Regents, ECAS performed a systemwide audit of foreign influence in coordination with the campus internal audit departments. This audit was identified as a key component of the University's systemwide compliance plan for foreign influence.

Most of the audit work involved interviews with relevant campus personnel to gain an understanding of processes, controls, and monitoring mechanisms in place to mitigate

risks associated with foreign influence, as well as processes in place to identify and respond to noncompliance with required disclosures related to conflicts of interest, conflicts of commitment, and other support, including:

- Training and awareness programs,
- How positive disclosures are handled/managed,
- Monitoring and/or reconciliation of disclosure information,
- Third-party screening,
- Escalation procedures when discrepancies or other concerns are identified,
- Record keeping procedures, and
- Mechanisms to secure pre-publication data and research space.

Additionally, the auditors selected a sample of NIH grants and compared information in grant documents, sabbatical records, and publications to evaluate the accuracy of other support and affiliation reporting.

The audit identified several areas where ECAS could partner with RPAC and UC Legal to strengthen existing processes and practices. Specifically, ECAS will work with its research partners to develop institutional protocols to minimize the risk of inaccurate or incomplete information related to foreign research support, foreign talent programs, and affiliations of key personnel in contract and grant proposals, targeting high-risk cases. ECAS will also create guidance for local procedures for identifying red flags in agreements, restricted party screening, vetting international scholars, and appropriate local escalation. The implementation of these recommendations will augment ECAS's research and export control-related efforts currently underway.

## Artificial Intelligence

President Drake formed a presidential working group that is charged with developing overarching ethical principles and guides for the University's current and future use of AI. The presidential working group is currently developing UC ethical AI principles to guide the development and application of AI in ways consistent with UC's mission and values. The final report, due November 2021, will also provide recommendations to President Drake regarding best practices and guidance to:

- Develop methods and mechanisms to operationalize the UC ethical AI principles in the use of existing AI systems and the development of new applications of AI within the UC system, especially in areas likely to impact

individual rights, including health, human resources, policing, and student experience.

- Create the foundation for a permanent council that will further the principles, standards, methods, and mechanisms developed by this working group to counter the potentially harmful effects of AI and strengthen positive outcomes within the UC system.
- Make further recommendations on appropriate data stewardship standards for UC data that may be used in the development and use of AI-enabled tools and systems.

## B. EXPORT CONTROL

Many aspects of the University's operations include an international component that requires export control considerations. ECAS coordinates with Export Control Officers (ECOs) at the campuses to build awareness throughout the system and ensure compliance with these complex regulations.

### REGULATORY ENVIRONMENT

Export control laws regulate the distribution of items, information, software, and services to foreign nationals, foreign countries, and restricted entities. While export controls can cover a number of areas, the three key regulatory regimes are:

- The Export Administration Regulations (EAR), implemented by the Bureau of Industry and Security (BIS) within the Department of Commerce. The EAR regulates the export of goods and services that are "dual use" (having both military and civilian uses) as identified on the Commerce Control List. These are primarily commercial items with potential military uses.
- The International Traffic in Arms Regulations (ITAR), implemented by the State Department's Directorate of Defense Trade Controls. These regulations apply to articles, services, and related technical data that are inherently military in nature, as determined by the State Department. These "defense articles," "defense services," and related "technical data" are listed on the U.S. Munitions List (USML).
- The Treasury Department's Office of Foreign Assets Control (OFAC), which implements economic and trade sanctions based on U.S. foreign policy and national security goals. OFAC sanctions target foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. The University typically

encounters issues arising under the OFAC regulations when researchers engage in collaborations with foreign nationals overseas or seek to teach classes or perform research in foreign countries.

The federal government also maintains lists of individuals, organizations, and companies whose activities are contrary to U.S. national security, economic, or foreign policy interests. Federal law prohibits the UC from engaging with individuals and entities on these denied party lists in some cases.

Violations of export control regulations may result in institutional liability and substantial penalties. The federal agencies responsible for export control regulations include the Departments of Commerce, State, Treasury, and Energy, the Nuclear Regulatory Commission, and others.

## KEY PROJECTS

### Training and Professional Development

In order to improve awareness of export controls, and to address risks identified in the foreign influence audit, ECAS will develop a series of trainings in FY 2021-22, including:

- An interactive and customizable online course focusing on export control related issues and risks for University staff and faculty across the system. The course will be available to all UC locations in their respective learning management systems.
- An online training course related to restricted parties and the UC's Restricted Party Screening (RPS) tool that will inform UC staff and faculty what a restricted party is, how, and when to screen for such relationships, and where individuals can get assistance.
- A suite of advanced export classification training for location ECOs to further develop their skills in regulatory interpretation and application.

Additionally, the federal government identifies foreign individuals and organizations that are on restricted lists and requires applicable licensing exceptions for any interactions with these individuals and/or organizations. ECOs within the system commonly review the legal requirements related to these interactions. Any additional compliance or reputational risks are evaluated separately. ECAS will assist the Vice Chancellors for Research to strengthen screening processes related to these engagements. These screening processes will include developing restricted party escalation guidance for locations, ensuring that campus leadership have relevant information before entering into these relationships.

ECAS is working with location stakeholders to develop other tools, including:

- A risk maturity model tool to allow ECOs to better assess and address gaps and growth within their compliance programs.
- Updated technology control plan templates that can be customized by locations for their use.

### ITAR Compliance Program Maturity

The International Traffic in Arms Regulations (ITAR) control military-related items and services as part of international, multi-lateral arms agreements. U.S. organizations that possess or export defense items or provide services must register with the Department of State and get approval for these activities. A small number of UC operations and research require the use and occasional export of these controlled items. ECAS is designated as the empowered official to hold and manage the ITAR registration for the entire system. During this FY 2021-22, ECAS will be working to improve ITAR compliance standardization across the system in an effort to promote continuous improvement. For example, ECAS will work with the Vice Chancellors for Research to create more standardized management support statements. Management support statements communicate to the UC community our leadership's commitment to compliance with federal export controls, and are an important element of a compliance program under State Department guidelines.

### Industrial Security

At UC, a small number of key leadership and staff hold a U.S. government security clearance. The federal government requires that these "cleared personnel" receive regular training on the security principles related to the protection of sensitive information. ECAS has developed a security program at the system level that ensures the appropriate training occurs for these cleared personnel.

The federal government also requires UC to continually evaluate and assess the appropriateness of these clearances, especially when new and relevant information becomes available. ECAS is currently establishing processes and procedures to perform these evaluations, by coordinating with UC Legal and leveraging existing investigative functions.

This initiative will satisfy federal requirements and ensure that UC's mission and partnership with federal agencies continues uninterrupted.

## C. HEALTHCARE COMPLIANCE AND PRIVACY

UC's academic medical centers (AMCs) and their operations are some of the most complex and heavily regulated entities within the system. HCCOs at each location assist leadership in identifying and navigating the highest-risk activities throughout their

respective AMCs through the development and execution of risk assessments and compliance plans. These risk assessments and related compliance plans also identify shared risks amongst the AMCs and inform ECAS's efforts for the year. As detailed below, in collaboration with UC Legal, ECAS works closely with locations to coordinate common efforts for shared risks, provides necessary awareness and training activities for new or emergent regulations, and identifies best practices to mitigate these shared, high-risk activities.

## REGULATORY ENVIRONMENT

Healthcare compliance obligations largely center around laws designed to protect government health programs (e.g., Medicare and Medicaid) from fraud and abuse. The following are some of the core laws related to healthcare compliance:

- The False Claims Act (FCA) protects the federal government from being overcharged or sold substandard goods or services. Examples of potential violations include billing services that did not occur, billing for higher paying services than services rendered, incorrect coding, or over-ordering of services.
- The Physician Self-Referral Law (Stark Law) prohibits a physician from referring patients to receive certain health services payable by Medicare or Medicaid to an entity with which the physician or a member of the physician's immediate family has a financial relationship (certain exceptions apply).
- The Anti-Kickback Statute (AKS) makes it a crime to knowingly and willfully offer, pay, solicit, or receive any remuneration to induce or reward patient referrals or any generation of business involving services reimbursable by a federal health care program. Remuneration includes anything of value, such as cash, complimentary rent, meals, hotel stays, or excessive compensation for medical directorships or consultancies.
- The Health Information Portability and Accountability Act (HIPAA) creates privacy standards for safeguarding electronic personal health records.

## KEY PROJECTS

### Risk Assessments

ECAS recently collaborated with the HCCOs to implement a shared methodology for assessing and addressing high-risk activities at the AMCs. Each location's process included the use of surveys and interviews with senior leadership throughout the medical centers and schools of medicine. ECAS will be working closely with UC Health and AMC leadership to strengthen the risk assessment process to further assist leadership in identifying, tracking, and mitigating compliance efforts at their respective locations.

## Oversight of Revenue Cycle Compliance

The AMCs regularly treat thousands of patients each year and must accurately translate those services into medical codes to obtain reimbursement from private insurance carriers or federal programs. If the medical codes are improperly submitted, an AMC's reimbursement could be delayed or even denied, resulting in lost revenue. In more serious cases, these errors could result in allegations of fraud, significant legal costs and penalties, loss of reputation, and possible criminal penalties. For example, if an AMC mistakenly files incorrect claims to the government, there may be a violation of the Federal Civil False Claims Act (FCA). Because of these issues and the potential liability, the AMCs routinely rank these issues among their highest risks.

Each of the AMCs have a dedicated oversight team to review revenue cycle-related issues. ECAS will continue to convene the HCCOs and UC Legal on a monthly basis to review significant changes to billing and coding standards as well as alerts and guidance from the Centers for Medicare and Medicaid Services (CMS), the U.S. Department of Health and Human Services (HHS) Office of the Inspector General (OIG), and private insurance carriers.

ECAS's compliance efforts for FY 2021-22 will also focus on the procurement and implementation of a common audit software program to be used throughout the system. This common software will, among other things, allow ECAS and UC Legal to assist HCCOs in reviewing high-risk coding and billings areas in a uniform manner. This common platform and approach will augment the HCCOs' existing processes and will increase the locations' ability to identify and remediate potential issues.

## Conflicts of Interest and Commitment

Existing federal law and UC policies require faculty to disclose certain external sources of income or employment to the University. In an effort to strengthen existing processes, UC Health established a working group in 2020 to review the policies, practices, and systems related to disclosure of outside professional activities. The working group developed a series of recommendations to enhance existing policies and procedures, reporting mechanisms, and systems for evaluating outside professional activities.

In FY 2021-22, ECAS will be working alongside UC Health, the individual UC Health locations, and UC Legal to implement a number of these recommendations, including a revision to the existing UC Vendor Relations Policy that will delineate appropriate interactions and relationships between University personnel and vendors.

### Health and Clinical Research Data Management

Several privacy, security, and healthcare requirements, such as HIPAA, the General Data Protection Regulation (GDPR), the AKS, and UC security policies, are embedded in UC systemwide contract templates used to purchase information technology (IT) software, systems, and applications. Inconsistent use of existing templates, frequent contract term changes, and inconsistent application of relevant policies increase the risk of noncompliance.

Working with UC Legal, ECAS will review contract terms most commonly changed by vendors, which could lead to noncompliance. ECAS will develop training and tools to enable UC staff to more efficiently navigate negotiations and ensure that contracts are compliant with relevant policies.

ECAS will also continue to provide guidance to relevant stakeholders and create training materials to raise awareness of compliance risks associated with data sharing agreements.

ECAS training materials for this fiscal year will focus on:

- Ensuring that vendors provide clear data sharing requests and outline data uses for compliance professionals to evaluate any limitations the University may need to impose on the use of data.
- Providing guidance to minimize the use of personally identifiable data in data sharing agreements by removing identifying elements.
- Ensuring appropriate authorizations are obtained prior to execution of data sharing agreements.

### Cybersecurity

A cybersecurity attack on a hospital system can devastate its operations by potentially shutting down entire medical record systems and life preserving medical equipment, risking significant patient harm. In June 2021, the HHS OIG identified cybersecurity oversight for networked medical devices in hospitals as an area of concern suggesting future focus on these issues. To help minimize the likelihood of an attack, and to ensure readiness for such an event, the ECAS Cybersecurity Audit Team (CAT), in consultation with the ECAS healthcare compliance team, will review the AMCs' incident response, disaster recovery, and continuity plans and procedures, and assess their overall preparedness to respond to and recover from a major cyber-attack.

## D. CAMPUS PRIVACY

Campus privacy programs ensure the appropriate protection, use, and release of student, faculty, staff, and research participant information. Privacy compliance at the University

balances the dual aims of maintaining an open and robust academic and research environment, and ensuring the University's vast amount of sensitive data is safeguarded.

ECAS participates in and provides expertise to multiple cross-functional privacy and security committees. ECAS also convenes the Systemwide UC Campus Privacy Officers Group. To address uneven resources and support available at each campus, the systemwide privacy group works to harness the unique expertise and resources available at each location to jointly address common areas of concern.

## REGULATORY ENVIRONMENT

The Family Educational Rights and Privacy Act (FERPA), California Public Records Act (CPRA), and California Information Practices Act (CIPA) are the predominant privacy requirements campuses are subject to, while locations treating patients or performing research must also oversee compliance with HIPAA, the CMIA, the Food and Drug Act, and GDPR. All privacy requirements subject the University, and in some cases its employees, to possible government fines, enforcement actions, and reputational harm. A violation of FERPA, for example, may result in loss of federal funding.

The regulatory environment in the area of privacy has become more complex in 2020, in part due to widespread use of big data, mining of personal data, and implementation of the California Consumer Privacy Act (CCPA) and its November 2020 companion, the California Privacy Rights Act (CPRA[1]). Several other pending legislative initiatives propose additional safeguards for the use of health, genetic, and human subjects' research data.

## KEY PROJECTS

ECAS and the Campus Privacy Officers have identified the following systemwide priorities for FY 2021-22: the development of a model framework for privacy programs at UC locations, the strengthening of coordination between privacy and IT security teams, and the privacy implications of campuses re-opening.

### Privacy Framework

ECAS and the Campus Privacy Officers will create a common privacy framework for UC that will allow locations to evaluate their current programs against best practices. The framework will identify key elements of an effective higher education privacy program, the graduated stages of program maturity (from minimally to fully developed), and the related level of risk associated with each level. The framework will enable campuses to conduct a baseline assessment of their current programs and facilitate risk-based discussions with their leadership on how to best right-size their programs and apply limited resources to the key issues.

### Coordination between Privacy and IT Security Teams

The University's Campus Privacy Officers and Chief Information Security Officers (CISOs) have overlapping objectives related to management of sensitive data. It is incumbent upon both privacy and security officers to collaborate closely in order to effectively safeguard the University's data. One such area of intersection involves the University's Electronic Communications Policy (ECP[2]). The ECP is a presidential policy that establishes rules and procedures for all electronic communications at the University, including (a) privacy, confidentiality, and security in electronic communications, (b) appropriate use of electronic communications, and (c) the use of electronic resources in compliance with laws and University policies. Although technology and privacy related regulations have evolved rapidly in recent years, the ECP has not been modified since 2005. ECAS will closely collaborate with IT and Campus Privacy Officers in modernizing the ECP to ensure appropriate technology, security, and privacy issues are addressed.

### Campus Re-Opening

Most University locations have been operating in a remote environment since 2020. ECAS, in collaboration with Campus Privacy Officers, HCCOs, UC Legal, and UC Health, contributed to a number of pandemic-driven initiatives over the past year. As campuses begin to reopen for faculty, research facilities, and staff, ECAS will continue to identify compliance risks related to privacy of data, including new and anticipated regulatory changes.

Each location established a cross-functional team to prepare for re-opening. The teams' focus will be to ensure that compliance with existing and new federal, state, and local requirements is integrated during re-opening of different functions such as education, administration, and housing. ECAS will participate in these efforts to address existing and emergent compliance risks.

## E. CLERY ACT COMPLIANCE

The University's Clery Act compliance program is managed by Clery Act officers or coordinators at each location. In accordance with Clery Act requirements, each campus publishes an annual security and safety report, including crime statistics, information on various campus and community resources related to crime prevention, and community assistance. The resources dedicated to this area vary across the system, but the locations work together to identify high-risk areas, leverage best practices and pursue opportunities to strengthen the systemwide program.

## REGULATORY ENVIRONMENT

The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Act) of 1998 is part of the Higher Education Act. The Clery Act statute requires colleges and universities participating in federal financial aid programs to maintain and timely disclose campus crime statistics and security information to the University community. The Clery Act also requires campuses to report these statistics annually to the U.S. Department of Education.

In 2019 and 2020, the federal government levied record-high Clery Act fines against two universities across the country, including one UC campus, for inappropriate reporting, ineffective systems for collecting crime statistics, and failure to issue timely warnings to the campus community.

## KEY PROJECTS

### Training and Professional Development

ECAS will continue to regularly convene meetings with Clery Act officers and coordinators throughout the system to ensure awareness and coordination on these issues.

ECAS will provide routine guidance and training to individual campuses throughout the system. In FY 2021-22, ECAS will develop an in-depth course for Clery Act compliance professionals in conjunction with a nationally recognized Clery Act expert focusing on established best practices and dissecting new issues:

- California requirements for reviewing crime classifications and geography.
- Reporting responsibilities for Campus Security Authorities (CSAs), including essential reporting elements of the crimes they must report, filing requirements, and institutional responsibilities regarding ongoing disclosures to the campus community.
- Recent changes to the Violence Against Women Act expand key provisions of the Clery Act; the session will focus on the types of crime mandated for Clery Act reporting.

In November 2021, ECAS will deliver the annual Clery Act training tailored to the UC campuses and AMCs' unique environments. The course will give an overview of current risks and provide practitioner training for Clery Act professionals responsible for day-to-day Clery Act compliance operations.

### Compliance Assessment

ECAS is engaging a national expert to conduct an assessment of UC Office of the President (UCOP) properties to determine if UCOP needs a Clery Act compliance function separate from its existing shared arrangement with UC Berkeley. The review will conclude in mid-2021. ECAS will develop a UCOP Clery Act Compliance Plan for FY 2021-22 based on the assessment findings.

### CSA Working Group

The CSA Identification working group will continue to evaluate the methodology used to identify CSAs at each location, as required by the UC Clery Act Policy and the federal Clery Act. The working group will include analysis of systemwide data examining job codes, job descriptions, reporting structure, and level of involvement with students. The working group will develop a report with a baseline CSA list which can be expanded by each location. The working group is also engaging experts across the system to identify other potential methods for systematically flagging employees who meet the CSA criteria (e.g., UCPath CSA functionality).

## F. AMERICANS WITH DISABILITIES ACT (ADA) COMPLIANCE

ECAS recognizes ADA compliance as a risk priority for the system because of the breadth of issues and persons affected by these regulations and the potential reputational and fiscal harm of noncompliance. During FY 2020-21, ECAS created a new ADA compliance coordinator role to enhance the systemwide capabilities regarding ADA compliance and increase awareness through the development of systemwide communications, training, and educational materials.

### REGULATORY ENVIRONMENT

ADA compliance at UC is an umbrella term encompassing systemwide compliance with disability-related laws, regulations, and guidance at both the federal and state level. Federally, UC is subject to the broad requirements of the ADA and Section 504 of the Rehabilitation Act (among others) prohibiting discrimination on the basis of disability by ensuring that entities receiving federal funds are equally accessible to individuals with disabilities. These federal regulations are generally enforced by the Department of Justice, the Office of Civil Rights, and/or the Equal Employment Opportunity Commission. California has enacted additional, and often broader, regulations around disability including the California Fair Employment and Housing Act, the Unruh Civil Rights Act, and the Disabled Persons Act – all enforced by the Department of Fair Employment and Housing. Moreover, many federal and state regulations similarly allow for civil enforcement by litigants. The UC is also subject to the disability civil rights compliance programs set forth by federal funding agencies such as the NSF.

This regulatory framework affects UC campuses, AMCs, laboratories, and other UC facilities, and all aspects of the services, programs, and activities conducted at each location.

## KEY PROJECTS

For FY 2021-22, ECAS's ADA compliance efforts will focus on stakeholder engagement and benchmarking activities. ECAS will create an ADA compliance webpage to link the campus compliance efforts in this area and to maintain current information on the regulatory frameworks at play and relevant ECAS and campus guidance.

ECAS will begin drafting training and education materials focusing first on ensuring awareness of best practices in the provision of academic accommodations. ECAS will also create similar guidance on employment accommodations to increase awareness of UC's obligations in that arena.

ADA requires UC campuses, AMCs, and other locations to designate at least one responsible employee to coordinate ADA compliance. Each ADA coordinator is responsible for coordinating the efforts of their campus to comply with the ADA and investigating any complaints that the campus has violated Title II[3] of the ADA. ECAS will develop best practices on the roles and responsibilities of an effective ADA coordinator as a mechanism for level-setting within the UC system.

## III. ENDNOTES

[1] California Privacy Rights Act: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=7.&chapter=3.5.&lawCode=GOV&title=1.&article=1

[2] Electronic Communications Policy: https://policy.ucop.edu/doc/7000470/ElectronicCommunications

[3] Title II of the ADA: https://www.govinfo.gov/content/pkg/USCODE-2009-title42/html/USCODE-2009-title42-chap126.htm