UNIVERSITY OF CALIFORNIA

OFFICE OF ETHICS, COMPLIANCE AND AUDIT SERVICES

COMPLIANCE ALERT

This Issue's Contents

Here's What's Happening at ECAS 1
Audit and Investigations 2
Cybersecurity 2
General Compliance 2
Health Sciences Compliance 3
International Compliance 3
Research Compliance 4
Policy 4
Privacy 4

Here's What's Happening at ECAS

- New ECAS Compliance Team: ECAS welcomes the following individuals:
  - D'Arcy Myjer as the new Director of Compliance. Most recently, D'Arcy was the Director of Compliance for Delta Dental of California and before that he managed the shared services HIM Departments for Stanford Hospital and Lucile Packard Children's Hospital and served as the first HIPAA Privacy Officer for both hospitals and the medical school.
  - Scott Seaborn as the new Privacy Compliance Manager. Scott has over 6 years of previous experience as a Privacy Officer. In addition he has over 15 years of experience in other areas such as FDA, HHS/OIG compliance, healthcare and operational audit, OCR, EEO, and other general compliance areas. Scott has experience working in a public agencies and as an auditor UCSF and for UCOP.
  - Nicole Delange as the new Healthcare Compliance Manager. Most recently, Nicole worked as a compliance manager for the Palomar Health System, a role into which she was promoted starting as an Administrative Fellow. She has a range of compliance experiences, including redesigning the Code of Conduct, work processes on fair market value, and auditing billing practices.
  - Shanda Hunt as the new Research Compliance Manager. Shanda comes to this role with more than 10 years of experience in variety of roles, including research contracts and grants for UCSF and UCB, operations analysis for the City of San Francisco, Assistant Director for the Center for Environmental Research and Children's Health at UC Berkeley, and as a program manager and HR compliance analyst for UCOP, Systemwide Human Resources.
- General Compliance Briefing Update

  The updated online course is available starting March 2018. Each UC location will determine the exact rollout. The briefing does not teach ethics or policy. Instead, the goal of the briefing is to raise awareness of the University of California Statement of Ethical Values and Standards of Ethical Conduct and also conveys University employment obligations with respect to ethical and compliant behavior. The course is also available in Spanish.
- Upcoming Educational Opportunity

  ECAS is pleased to announce an upcoming two-day training on conducting workplace investigations at UC. The training will be held June 26-27 in Oakland. Please register soon as room capacity is limited.
- Compliance Alert Updated Format

  This reformatted ECAS newsletter has been redesigned to better accommodate Web Content Accessibility Guidelines (2.0) and to make web content more accessible to audience members with disabilities.

Audit and Investigations

ED Interest in Data Security Ramps Up

The Federal Student Aid (FSA) division of the Department of Education sent compliance letters to universities and colleges expressing concerns over suspected data breaches. Previously, FSA indicated they are interested in auditing higher education institutions data protection and information security.

Office for Civil Rights Issues Updated Case Processing Manual

Effective March 5, 2018, the Department of Education's Office for Civil Rights released an updated Case Manual. Updates include reduced response timeframe for complainants, limiting investigations into possible systemic issues at schools, and expanding the circumstances for dismissal of investigations.

Cybersecurity

Don't Let a Phishing Scam Reel You In

Cybercriminals use phishing—a type of social engineering—to manipulate people into doing what they want. Social engineering is at the heart of all phishing attacks, especially those conducted via e-mail. Technology makes phishing easy. Setting up and operating a phishing attack is fast, inexpensive, and low risk: any cybercriminal with an e-mail address can launch one.

The education sector has seen a rise in social engineering–based attacks. Students, staff, and faculty all suffer losses when personal data and research are disclosed to unauthorized parties. Phishing played a part in more than 40% of these breaches. Knowing what you are up against can help you be more secure. Here are a few things you can do to guard against phishing attacks:

- **Limit what you share online.** The less you share about yourself, the smaller the target you are for a phishing attack. Cybercriminals use information you post online to learn how to gain your trust.
- **Protect your credentials.** No legitimate company or organization will ask for your username and password or other personal information via e-mail. The University definitely will not. Still not sure if the e-mail is a phish? Contact your IT help desk.
- **Beware of attachments.** E-mail attachments are the most common vector for malicious software. When you get a message with an attachment, delete it unless you are expecting it and are absolutely certain it is legitimate. If you are not sure, call the sender at a number you know belongs to them to check.
- **Confirm identities.** Phishing messages can look official. Cybercriminals steal organization and company identities, including e-mail addresses, logos, and URLs that are close to the links they're trying to imitate. There's nothing to stop them from impersonating the university, financial institutions, retailers, a wide range of other service providers, or even someone you know.
- **Trust your instincts.** If you get a suspicious message that claims to be from an agency or service provider, use your browser to manually locate the organization online and contact them via the website, e-mail, or telephone number that you looked up – not what was provided in the message.
- **Check the sender.** Check the sender's e-mail address. Any correspondence from an organization should come from an organizational e-mail address. A notice from your college or university is unlikely to come from IThelpdesk@yahoo.com.
- **Take your time.** If a message states that you must act immediately or lose access, do not comply. Phishing attempts frequently threaten a loss of service unless you do something. Cybercriminals want you to react without thinking; an urgent call to action makes you more likely to cooperate.
- **Do not click links in suspicious messages.** If you do not trust the e-mail (or text message or post), do not trust the links in it either. Beware of links hidden by URL shorteners or text like "Click Here." They may link to a phishing site or a form designed to steal your username and password.

For other effective cybersecurity habits, check out UC's "Make It a Habit" webpage.

Additional resources are available through a Phishing Awareness Toolkit on the Systemwide Information Security website.

General Compliance

Why Compliance Programs Fail – and How to Fix Them

Government regulators continue to evaluate institutions based on the presence of a compliance program, alignment of policy with government regulations and the use of compliance metrics.

New Presidential Task Force on University Police Departments

During UC President Napolitano's opening remarks at the March 14 Board of Regents meeting, she announced that Senior Vice President and Chief Compliance and Audit Officer Alex Bustamante will chair a new task force to review university police department processes and practices.

Health Sciences Compliance

Consequences for HIPAA Violations Don't Stop When a Business Closes

FileFax, a business that stored, maintained, and delivered medical records, closed its doors after an investigation by Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and allegations of HIPAA violations. However, when OCR learned, through an anonymous complaint, that FileFax continued to mishandle the disposal of medical records containing protected health information, it fined FileFax an additional $100,000.

Five Breaches Add Up to Millions in Settlement Costs for Entity that Failed to Heed HIPAA Rules

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) reached a $3.5 million agreement with the Fresenius Medical Care North America (FMCNA) organization for five breaches since 2013 that put patient protected information at risk.

International Compliance

Updated Guidance: International Travelers with Mobile Devices

Mobile devices pose risks to UC personnel when traveling internationally. Privacy and security protections vary by country and often fall short of the protections against governmental access we expect in the U.S. This means that foreign border security may seize or access a laptop and its contents, including making backups.

At US borders, security has tightened as the courts are hearing cases limiting the applicability of the fourth Amendment's guarantees against unreasonable search and seizure. Trends:

- In FY 2012, US Customs and Border Patrol (CBP) reported 5,085 device searches.
- By fiscal year 2015, CBP searched the electronic devices of 8,503 international travelers.
- In FY 2017, the number increased to 30,200—a six-fold increase in just five years. (Click here for more information.)

As an individual traveler, one of the best protections against device searches, information thieves, or viruses is to use a "travel laptop." Travelers to "at risk" countries should work with their campus IT departments to borrow a laptop, which only holds the information needed for that trip and which can be completely wiped on return to eliminate the risk of malware. Vulnerable and valuable data and controlled information should remain safely at home.

In planning a trip, UC travelers should ask themselves:

- Am I carrying any information or data which is proprietary or under a non-disclosure agreement?
- What are the consequences if this information is compromised?
- Is the information controlled in any way including PHI, PII, PCI, or CUI?
- Is an Export license required to take this information out of the country?
- Do I know the rules for entering my destination country as well as planned and potential layover countries?
- Will my travel itinerary cause scrutiny by US Custom Officials as I re-enter the country.
- Is the information and data contained on the device more valuable than the device itself?

International travelers should contact their local Export Control Leads and IT Security personnel to discuss any concerns and to safeguard their work. Useful links for more information:

- Export Control Contacts
- Guidance from UCGO
- Traveling with Electronic Devices

Tools: eCustoms' Visual Compliance

Visual Compliance is a powerful set of tools for faculty, administrative staff and compliance teams. The cloud based solution is available at each campus and should be used for Restricted Party Screening (RPS), Commodity Classification, and Controlled Technology Management.

For (RPS) screening, Visual Compliance helps ensure overseas vendors, colleagues, and other foreign (and domestic) contacts are not flagged on any US Government Denied Party, Sanctions, or Embargo lists. Visual Compliance is updated daily and a single entry will provide a consolidated screening against the Commerce Department's Bureau of Industry and Security's Denied Persons lists, comprehensive OFAC watch lists, Sanctions and Embargoes and other lists.

One of the great features of the product is that if an individual or entity is screened once and cleared, but later added to a government list, the original screener will be notified of the change and can revisit the matter.

Another tool within the Visual Compliance application is the Commodity Classification Tool, which allows users to understand what controls apply to hardware, software, and other categories of technology. This is especially important when considering sending technology overseas or when sharing information.

ECAS offers regular training on this application and you may also request individual help by contacting Brian Warshawsky at Brian.Warshawsky@ucop.edu. Local Export Control Officers are also a great resource and ECAS recommends working closely with your local expert.

Research Compliance

NSF Notice Requiring Grantee Organizations to Report PI Harassment Findings

The National Science Foundation (NSF) announced it intends to require colleges, universities, and other institutions to report NSF-funded researchers and other grant personnel facing allegations of harassment of any kind. In addition, the NSF Office of Diversity and Inclusion will integrate resources into a web portal dedicated to providing information concerning harassment to the research community.

Facebook Fallout

Facebook's platform permits third party developers, including academic researchers, to retrieve user data. A Cambridge University researcher obtained a large amount of data for academic research, but shared the information without Facebook and user permission.

Policy

New UC Policy

Unmanned Aircraft System (Drone) Policy:

The purpose of this Unmanned Aircraft System (UAS) Policy is to establish University oversight and minimum record-keeping requirements for UAS, commonly known as drones and includes Small Unmanned Aircraft Systems (SUAS) and model aircraft. This policy requires that all UC UAS operations perform in a manner that mitigates risks to safety, security, and privacy, and ensures compliance with all applicable laws. This includes, but is not limited to regulations regarding US domestic airspace, international airspace, aircraft registration, and state or other local regulations.

Recent UC Policy Updates

Discrimination, Harassment, and Affirmative Action in the Workplace:

Effective February 14, 2018, this policy has undergone the following changes:

- Deleted definition of "Covered Veteran" and added definition of "Protected Veteran" to comply with the Vietnam Era Veterans Readjustment Assistance Act, as amended (VEVRAA) (41 CFR 60-300.2)
- Modified definitions of "Gender Expression" and "Gender Identity," and added definitions of "Gender Transition," "Sex," and "Transgender" to comply with definitions in 2 CCR § 11030
- Updated for compliance with California Fair Employment and Housing Act regulations regarding Harassment and Discrimination Prevention and Correction (CCR § 11023)
- Updated for compliance with California Assembly Bill 1443, which extends discrimination and harassment protections to volunteers, unpaid interns, and trainees, and harassment protections to contractors (2 CCR § 11009, 11019)
- Added pay transparency Nondiscrimination Provision required by the Office of Federal Contract Compliance Programs (41 CFR 60-1.35(c))
- Reformatted Policy Statement with subsections
- Added reference to the University's Sexual Violence and Sexual Harassment policy in Section III.A

Presidential Guidelines

Presidential Guidelines Governing the UCOP Strategic Priorities Fund:

As part of its standard budgeting practices, University of California Office of the President should maintain a Strategic Priorities Fund to support funding for one-time and limited-term strategic priorities and projects and urgent, emerging issues.

Presidential Guidelines Governing the UCOP Central Operating Reserve:

This guidelines document provides additional detail related to the Regents Central Operating Reserve policy:
The Regents require that the University of California Office of the President (UCOP) maintain a Central Operating Reserve to support operations in the event of an unanticipated disruption in planned funding. The University of California Office of the President shall specify and document the size and funding source(s) for the Central Operating Reserve in a guidelines document to be posted on the UCOP website.

Privacy

Why Care About GDPR?

Following an EDUCAUSE webinar on the General Data Protection Regulation (GDPR), questions arose on why higher education institutions should prepare for the new European law. The main drivers for compliance lie in how colleges and universities interact with European regulators, partners, and students. For more information, review the EDUCAUSE GDPR articles and resources. UCOP will communicate more guidance shortly.

Patient Data on Phones Introduces New Privacy and Security Concerns

New applications, which allow patients to download their health information onto their phones improves access, but increases privacy vulnerabilities. Academic medical centers working with application vendors should design their mobile device applications to ensure compliance with HIPAA security and privacy controls and protect their patients from an inadvertent breach of Protected Health Information.