COMPLIANCE ALERT

Brought to you by: Ethics, Compliance and Audit Services

UNIVERSITY OF CALIFORNIA

This Issue's Contents

Audit and Investigations

UC Responds to State Audit Report on University of California Office of the President

Concerning a recent state audit report on University of California's Office of the President, the Board of Regents and UC's President have responded to the recommendations suggested by the California State Auditor. In addition, further information is provided in regards to the Office of the President's budget practices and presidential initiatives.

ED Proposes Auditing Safeguards Rule Compliance

The Department of Education (ED) is considering requiring compliance to the Safeguards Rule for audits concerning student financial aid. The Safeguards Rule under the Gramm-Leach-Billey Act requires financial institutions, such as universities, identify security risks and develop an information security plan in order to protect student information. It is expected that the Office of Management and Budget (OMB) will update their guidelines to include compliance with the Safeguards Rule when student financial aid information is audited. According to a recent update, the OMB is considering the new audit provision for 2017-2018.

Cybersecurity

Systemwide NIST Cybersecurity Framework Assessment Project

In September 2016, at the direction of UC's Cyber-Risk Governance Committee (CRGC), the Office of Ethics, Compliance, and Audit Services (ECAS) and the Cyber-Risk Coordination Center (C3) partnered to launch a systemwide cybersecurity risk assessment against the National Institute of

Here's What's Happening at ECAS

- The search for a new Senior Vice President and Chief Compliance and Audit Officer (SVP-CCAO) is underway. The SVP-CCAO position is posted and further information for applicants is available through the following link: UCOP SVP-CCAO Job Details.

- ECAS welcomes Vanessa Ridley as the new Director of Healthcare Compliance and Systemwide Privacy. The UCOP Health Sciences Compliance Program provides guidance for the development, implementation, and evaluation of all health science activities and functions spanning all university locations.

- The search for the new UCOP Director of Research Compliance is nearing completion. The position is estimated to be filled by June.

- Presidential Policies In The Works:
  ◊ Clery
  ◊ Video Security/Safety
  ◊ Export Control
  ◊ Policy on Policies
  ◊ Environmental, Health, and Safety
  ◊ Hazardous Materials: Shipping and Transportation
  ◊ Unmanned Aircraft Systems (Drone)
  ◊ Electronic Information Security

- Ethics and Compliance Training
  ◊ General Ethics and Compliance Briefing online course update to be rolled out in the Spring.

- Additional, relevant UC Policies are being translated and will be made available in different languages. Further information forthcoming.

UNIVERSITY OF CALIFORNIA

Standards and Technology's Cybersecurity Framework (NIST CSF or "Framework") to capture UC's current state of cybersecurity efforts.

According to NIST: "The Framework is voluntary guidance, based on existing standards, guidelines, and practices for critical infrastructure organizations to better manage and reduce cybersecurity risk." Adoption of the Framework is a collaborative effort and gives an organization the basis for a common set of terms and methodologies.

All UC locations have completed their assessments. The results of these location assessments are being used to produce a systemwide roll-up report, identifying themes that will inform UC's overall risk profile as well as help the CRGC make risk reduction decisions and prioritize cybersecurity investments. The systemwide roll-up report is expected to be completed in early June. The Chief Information Officers and Chief Information Security Officers will meet face to face in late June to review the roll-up report and develop recommendations to be presented at the August CRGC meeting.

New Video on the NIST Cybersecurity Framework and the FTC

A new video provided by the Federal Trade Commission's Division of Privacy and Identity Protection illustrates how complying with the NIST Cybersecurity Framework creates alignment with the Federal Trade Commission's requirements concerning data security.

Digital Spring Cleaning

A good digital spring cleaning can help keep your devices and information safe and secure year round. It can also help improve the speed and performance of the devices and services you use, and reduce the risk that a hacker could access old information that you've forgotten about.

Here are a few tips for refreshing, renewing, and reinvigorating your cyber life:

1. Review you online accounts.
2. Update you devices.
3. Purge those files!
4. Make sure you're secure.
5. Tune up your online presence.
6. Back up your files.
7. Dispose of electronic devices securely.

General Compliance

Can Universities Foster a Culture of Ethics? Some Are Trying

Over the last several years, universities in the United States have created centralized ethics and compliance offices. These offices focus on similar issues and aim to make their institutions compliant to regulations and foster an ethical culture. In contrast, they can differ in how they are structured.

Health Sciences Compliance

Indiana University Health and HealthNet to Pay $18 Million to Resolve False Claims Act Allegations

The Department of Justice has settled with Indiana University Health and HealthNet in order to resolve allegations of violating an Anti-Kickback Statute. Both parties had allegedly entered a financial arrangement in which referring patients to Indiana University's hospital was advantageous to HealthNet. The services would then be billed to Medicaid, categorizing the actions as false claims under the False Claims Act.

Overlooking Risks Leads to Breach, $400,000 Settlement

In January 2012, a Colorado health center reported a breach of employee email accounts and 3,200 individual electronic protected health information records. The Metro Community Provider Network had not conducted a risk assessment prior to the breach and will have to pay $400,000 for potential noncompliance with the HIPAA rules.

No Business Associate Agreement? $31K Mistake

Since 2003, the Center for Children's Digestive Health had been providing protected health information to FileFax, Inc. for storage. An investigation conducted by the Office of Civil Rights found that no signed business associate agreement existed between both parties.

$2.5 Million Settlement Shows that not Understanding HIPAA Requirement Creates Risk

A wireless health services provider, CardioNet, reported the theft of a worker's laptop containing electronic protected health information (ePHI). The Office for Civil Rights found the company had insufficient risk processes and lacked finalized policies enforcing the HIPAA Privacy and Security Rules.

UC Moves to Shut Down Alleged Fraud Targeting Students

The University of California filed a motion for a restraining order against health care providers who allegedly used student healthcare information to write fraudulent prescriptions. Students were approached to participate in "clinical trials" and were asked to provide their heath insurance information. The university is contacting students whose health information may have been used to steal $12 million through false claims.

JAMA May 2nd Issue

A recent, themed issue of the Journal of the American Medical Association (JAMA) presents several articles focused on the growing issue of conflicts of interest in the medical profession and health care.

Texas Health System Settles Potential HIPAA Disclosure Violations

After a patient attempted to use fraudulent identification, Memorial Hermann Health System MHHS) issued a press release which disclosed the patient's name. Subsequently, the U.S. Department of Health and Human Services found MHHS had potentially violated the HIPAA Privacy Rule.

Human Resources Compliance

New Systemwide Title IX Coordinator

The University of California has established Kathleen Salvaty as the first Systemwide Title IX Coordinator. As part of the university's continued effort to address sexual violence and sexual harassment, the Systemwide Title IX Coordinator will oversee UC's prevention and response to sexual violence, sexual harassment, dating and domestic violence, and stalking. She can be contacted by email at kathleen.salvaty@ucop.edu.

Research Compliance

FCPA Information and Resources

For universities engaged in international activities such as hosting foreign delegations, international research collaborations, and activities involving foreign governments, ECAS has updated its Foreign Corrupt Practices Act (FCPA) Information and Resources webpage. Available for review is guidance on the nature of activities prohibited under the FCPA, pitfalls for universities, and red flags to recognize to identify concerns before they become an issue. Available for viewing are past compliance webinars as well as information on the Introl to Foreign Corrupt Practices Act interactive training available in the LMS Learning Management System.

Harvard Teaching Hospital to Pay $10 Million to Settle Research Misconduct Allegations

The Department of Justice reached a settlement with Brigham and Women's Hospital, a teaching hospital affiliated with Harvard Medical School, which will pay $10 million to settle allegations of research misconduct. The hospital and medical school notified the federal government of an investigation it was conducting against a stem cell lab that possibly fabricated and published misleading data.

Top Scientists Revamp Standards to Foster Integrity in Research

The National Academies of Sciences, Engineering, and Medicine have published their report titled "Fostering Integrity in Research" to update the scientific conduct standards set in a 1992 report. The 2017 report aims to improve research integrity and expand the understanding of what would be considered questionable behavior by researchers.

Under Fire, National Academies Toughen Conflict-of-Interest Policies

The National Academies of Sciences, Engineering, and Medicine will update their financial conflict of interest policies in response to increased criticism of potential conflicts among study panel members. Effective immediately, academies' staff will also be required to report any potential conflicts of interest. In addition, panelists for the academies will be named in draft and final reports.

Policy

Recent UC Policy Updates

Trademark Licensing Code of Conduct

This policy describes how goods bearing the names of the University or its campuses, abbreviations of these names, logos, mascots, seals, or other trademarks owned by UC must be produced under fair, safe, and humane working conditions. All goods bearing UC Trademarks must be produced or otherwise sourced only through companies authorized to place UC trademarks onto products.

UNIVERSITY OF CALIFORNIA

Privacy

Is Privacy the Price of Precision Medicine?

The development of analytical tools that allow doctors to administer customized health care to patients requires personal information to improve accuracy and effectiveness. However, some researchers believe such medical information is not easily de-identified to protect a patient's privacy.

Is Digital Connectivity Threatening Your Privacy?

A study conducted by the Melbourne Networked Society Institute looked at how current privacy regulations protect individuals and whether they are understood by internet developers and users. Through interviews, users were found to have increased concerns of their privacy when using the Internet of Things (IoT) services, or systems allowing interconnection between devices. Developers were also found to not fully understand the legal and compliance requirements for protecting privacy when user data is collected, stored, or used.

Privacy Should Still Matter

As modern technology continues to expand in the Information Age, the right to keep personal information private faces challenges. At Princeton University, university databases collect data every time a student uses a prox card. In this article, a student shares their perspective on the importance of maintaining privacy.

Unroll.me Service Faces Backlash Over a Widespread Practice: Selling User Data

A data firm sold information gathered from people's email inboxes to companies seeking consumer data. Unroll.me does not sell personal identifiable information, but is able to sell anonymous data it collects while still adhering to its privacy policy.

California Supreme Court: No, You Can't Hide Public Records on a Private Account

The California Supreme Court found state and local employees communicating official business through private devices and accounts are still subject to the California Public Records Act. Such communications are considered public records and can be publicly accessible if requested.

Facebook and Instagram Publicly Prohibit Surveillance of Users Following Coalition Demands

A coalition comprised of the American Civil Liberties Union of California, the Center for Media Justice, and Color of Change petitioned companies to ensure that their user data was protected from being used for surveillance. In response, Facebook and Instagram have updated their policies to ensure user data obtained from either social media platform is protected.

New USPS Service Lets You Digitally Preview That Day's Mail Delivery

The U.S. Postal Service has a new and free service that will send residential customers images of the mail they will receive for the day. Customers can use the service to identify stolen mail containing personal information that could be used to steal their identities. In contrast, a hacked account could help criminals steal items of value or contain sensitive information.

Handshake Deal

The Handshake platform allows university students to create profiles and connect with potential employers. Privacy concerns have risen as some student GPAs may have been shared with Handshake and made visible without their permission.

Upcoming Educational Opportunities

♦   June 1—External Audit Coordination (Webinar)

♦   TBA—2018 Compliance and Audit Symposium

UNIVERSITY OF CALIFORNIA