



COMPLIANCE ALERT

Brought to you by: Ethics, Compliance and Audit Services



[Audit](#) [Compliance](#) [Investigations](#) [Presidential Policies](#) [Contact](#)

This Issue's Contents

Audit and Investigations	1
Cybersecurity	1
Health Sciences Compliance	2
International Compliance	2
Research Compliance	2
Policy	3
Privacy	4

Audit and Investigations

[Rush University Medical Center Disputes OIG Findings It Owes Government \\$10.2M](#)

An audit conducted by the Department of Health and Human Services Office of Inspector General reported Rush University Medical Center received Medicare overpayments totaling \$10.2 million. In response, the academic medical center has assigned their compliance program to conduct a six-year assessment of patient claims and billings.

Cybersecurity

[Protect Yourself from Tax Scams](#)

Tax season is coming and fraudsters soon will be sending fraudulent e-mail messages that look like legitimate tax communications. Don't become another victim. The IRS estimates that identity thieves have already stolen more than \$11 billion in tax fraud since 2012.

Be on alert for the following:

- Any message asking for W-2 or other tax information.
- Authentic looking emails impersonating UC communications about accessing your W-2.
- Messages that look like they are from executive management requesting copies of employee W-2s for review purposes. See the [IRS alert from last year](#) about this scam.
- Messages that encourage you to click on links, ask for passwords, etc.
- Unexpected phone calls about such messages, or asking you to install software.

Here's What's Happening at ECAS

◆ As of November 17, 2017, Senior Vice President and Chief Compliance and Audit Officer Alex Bustamante has been appointed the interim Locally Designated Official (LDO) for the Office of the President and for the University of California System with regard to both the UC Whistleblower Policy and the UC Whistleblower Protection Policy.

◆ New Chief of Staff

ECAS welcomes back Irene Levintov, who has begun her role as Chief of Staff. She rejoins the Office of Ethics, Compliance and Audit Services team after serving as Deputy Controller in the County of San Mateo.

◆ Research Compliance Manager

ECAS is recruiting for a Research Compliance Manager to be responsible for the systemwide research compliance program. Further information available through this link: [UCOP Job Post—20180035](#).

◆ Healthcare Compliance Manager

ECAS has begun its search for a Healthcare Compliance Manager to manage compliance issues within the UC healthcare enterprise. Information for this position is available through this link: [UCOP Job Post—20180037](#).

◆ Privacy Compliance Manager

ECAS is recruiting for a Privacy Compliance Manager in charge of privacy related projects, policies, and procedures. Additional information available through the following link: [UCOP Job Post—20180039](#).



COMPLIANCE ALERT

Brought to you by: Ethics, Compliance and Audit Services



[Audit](#) [Compliance](#) [Investigations](#) [Presidential Policies](#) [Contact](#)

Protect yourself.

- To access your W-2 statement, go directly to UC's At Your Service or UCPath website (whichever your location uses) instead of clicking on a link in an email.
- Use known contact information to verify any request for W-2 or other tax information, even if it looks like it's from someone you know. For example, call them first.
- Do not reply to emails asking for your password or SSN.
- Familiarize yourself with the [IRS' current list of tax scams](#) so you recognize them.

But don't stop there!

Here are [eight important cybersecurity habits](#) to help protect your information, your family and your work. They'll also reduce your risk of getting scammed!

Resources:

- [Identity Theft Resources](#)
- [UC Systemwide Information Security Awareness website](#)
- [Simple Cybersecurity Tips for Staying Safe Online During Tax Time](#), from StaySafeOnline.org
- [IRS Taxpayer Guide to Identity Theft](#)—includes Spanish, Chinese, Korean, Russian and Vietnamese translations

Health Sciences Compliance

[Confusion, Different Priorities May Cause EMTALA Violations](#)

A study conducted by UC researchers interviewed hospitals and patient safety organizations to gather insight as to why Emergency Medical Treatment and Active Labor Act (EMTALA) violations occur. The federal law requires emergency departments who receive federal funding to properly screen, treat, stabilize, or transfer patients regardless of their ability to pay for medical services.

[OCR works with DOJ to Ensure Federally Funded Medical Center Provides Communication Services for Deaf and Hard of Hearing Patients](#)

After receiving complaints of potential violations of Title III of the Americans with Disabilities Act, the U.S. Department of Health and Human Services Office for Civil Rights conducted a compliance review of the University of Vermont Medical Center. The results found the academic medical center requires improvements to its communication practices such as by providing auxiliary aids for patients with impaired sensory skills.

[Failure to Protect the Health Records of Millions of Persons Costs Entity Millions of Dollars](#)

In 2015, the Federal Bureau of Investigation (FBI) notified 21st Century Oncology, Inc. (21CO) that an informant was given 21CO patient information obtained illegally from its network. The unauthorized disclosure of protected health information was determined to have affected over 2 million individuals. Due to the potential violations of HIPAA, 21CO will pay \$2.3 million to the U.S. Department of Health and Human Services Office for Civil Rights.

International Compliance

[Presumption of Declination with Voluntary Disclosure, Cooperation, and Remediation of FCPA Violations](#)

Deputy Attorney General Rod J. Rosenstein announced the codification of a pilot program into the U.S. Attorneys' Manual meant to enforce compliance with the Foreign Corrupt Practices Act (FCPA). The policy provides a possible avoidance from prosecution if a company voluntarily discloses a violation and meets additional conditions. The FCPA was enacted to increase transparency in accounting practices and prevent U.S. companies and institutions from making corrupt payments, offers, or unauthorized promises to foreign government officials.

The Office of Ethics, Compliance and Audit Services has additional FCPA-related information through the UCOP ECAS webpage titled: [FCPA Information and Resources](#).

In addition, previously held FCPA-related webinars have been archived and posted:

- [FCPA: Advanced Tools and Regulatory Update Webinar](#)
- [International Activities: 3rd Parties and the Risk of Corruption](#)
- [International Activities: Due Diligence and Tools](#)

Research Compliance

[The Importance of Timely Grant Closeout](#)

The National Institutes of Health's (NIH) Deputy Director for Extramural Research, Dr. Michael Lauer, describes the importance of meeting closeout due dates for NIH awards in order to reduce added fees for maintaining open accounts past the due date and ensure accurate final grant expenditure. Improper closure could affect future NIH funding and may include further corrective actions.



COMPLIANCE ALERT

Brought to you by: Ethics, Compliance and Audit Services



[Audit](#) [Compliance](#) [Investigations](#) [Presidential Policies](#) [Contact](#)

NIH Enforcement of Closeout Policies

The National Institutes of Health (NIH) will begin to strengthen enforcement of all policies and requirements related to the closeout of grants. Grant award recipients are expected to submit on-time and accurate final grant expenditure reports for the proper closeout of NIH awards.

Too Good to Be True

Southern Illinois University is undergoing in-depth investigations concerning vaccine research conducted by a former professor on human subjects without proper oversight by an institutional review board. The university is expected to raise compliance awareness and apply corrective action.

HHS Announces Interim Final Rule, Delaying the Revised Federal Policy for the Protection of Human Subjects

The U.S. Department of Health and Human Services has announced that an Interim Final Rule has been published on the Federal Register that delays the revised Common Rule, a federal policy concerning protections for human subjects, which was to take effect on January 19, 2018. The new effective date has been set for July 19, 2018.

Policy

New UC Policy

Clery Act Policy—Campus Safety and Security Reporting:

This policy applies to all University of California staff, faculty, and students. It applies to all UC Campuses, Medical Centers, Agriculture and Natural Resources, Office of the President, and the Lawrence Berkeley National Laboratory.

This policy describes roles and responsibilities for the University Community related to compliance with the Clery Act including legal requirements regarding crime reporting, awareness, and prevention. In addition, this policy meets Web Content Accessibility Guidelines (WCAG) 2.0.

Recent UC Policy Updates

BFB-BUS-43 Purchases of Goods & Services; Supply Chain Management:

This policy was updated on November 17, 2017 to:

1. Update definitions relating to exceptions for competitively priced goods and/or services contracts for more than \$100,000 annually;
2. Encourage competition even when an exception applies

and require documentation of the decision to apply for an exception;

3. Require approval when University templates not used;
4. Provide consultation from the Office of General Counsel for Public Records Act requests during a procurement process or if RFP cancelled;
5. Add policy relating to debarring suppliers;
6. Update dollar threshold applicable to Prevailing Wage Services;
7. Limit circumstances under which exceptions to “after the fact” Fair Wage/Fair Work are approved;
8. Provide that contract duration may not exceed ten years unless an exception to policy is approved;
9. Provide that price may not have less than a 25% weight when the Best Value evaluation method is used;
10. Update provisions pertaining to leases;
11. Increase low-value purchase ceiling to \$10,000 for individual purchases;
12. Update language applicable to purchases that are federally funded;
13. Generally update the policy’s language for consistency;
14. Eliminate most hyperlinks

In addition, this policy was remediated in accordance with Web Content Accessibility Guidelines.

Guidelines on Contracting for Services:

This guideline was remediated to meet Web Content Accessibility Guidelines (WCAG) 2.0. As a result of the issuance of these guidelines, the Guidelines for Contracting for Services, dated September 4, 2002 (technical revisions August 25, 2011 and December 13, 2013) is rescinded and no longer applicable.

PPSM-21 Selection and Appointment:

Policy changes effective as of December 20, 2017: California Assembly Bill 1008 will add a section to the California Fair Employment and Housing Act (FEHA) containing state-wide restrictions on an employer’s ability to make pre-hire and personnel decisions based on an individual’s criminal history, including a “ban-the-box” component. As a result, technical changes were made to bring policy into compliance with legal requirements.



COMPLIANCE ALERT

Brought to you by: Ethics, Compliance and Audit Services



[Audit](#) [Compliance](#) [Investigations](#) [Presidential Policies](#) [Contact](#)

Newly Adopted Guidelines

UC Independent Contractor Guidelines:

The purpose of this Guideline is to provide a summary of the criteria used to determine a worker's status under Internal Revenue Service (IRS) common law standards and details the penalties imposed by the IRS for the misclassification of workers as independent contractors.

To assist in the determination of a worker's correct status for tax purposes, a compilation of IRS rulings and a Classification Worksheet are included as Exhibits.

These Guidelines address federal tax compliance only. There are other state and federal laws regarding classification of workers as independent contractors or employees.

Privacy

Resources in Support of International Data Privacy Day and Data Privacy Month

In honor and support of International Data Privacy Day (January 28) and Data Privacy Month (January 28 - February 28), a mini-awareness toolkit on the [Systemwide Information Security Awareness webpage](#) has been created and includes privacy-related articles and videos.

Data Privacy and You

All of us exist in digital form on the Internet. When you're online you leave a trail of "digital exhaust" in the form of cookies, GPS data, social network posts, browser searches, and email exchanges, among others. Services that you don't even use may have information about you. And once something is online, it can be there forever.

It is important to ensure that the digital "you" matches what you intend to share. It is also important to keep what's private, private, for yourself and when you're sharing about others. Owning your online presence will help to protect your identity, finances, and reputation – both now and in the future!

Here are some specific steps you can take to protect your online information, identity, and privacy.

- **Use a unique password for each site.** That way, if one of your passwords gets compromised, the others are still safe. Use complex passwords and never share them. Using multi-factor authentication (MFA) wherever possible will help protect you even more.
- **Use a password manager.** Using an encrypted password manager to store your passwords makes it easy to access and use a complex, unique password for each site.
- **Know what you are sharing.** Check the privacy settings on all of your apps and social media accounts to ensure that they are set to share only what you want, with whom you want. Don't rely on the default settings.
- **Guard your birth date and telephone number.** These are key pieces of information used for verification, and you should not share them publicly. If an online service or site asks you to share this critical information, consider whether it is important enough to warrant it.
- **Keep your university and personal presences separate.** Use different accounts for each.
- **There are no true secrets online.** Use the postcard or billboard test: Would you be comfortable with everyone reading a message or post? If not, don't share it.

But don't stop there!

Also check out these [eight important cybersecurity habits](#) to help protect your information, your family and your work. They'll also reduce your risk of getting scammed!

For more information about protecting your security and privacy, visit: [security.ucop.edu](#) or [ucal.us/privacy](#).

E.U. Data-Protection Law Looms

With the upcoming May 2018 implementation of the European Union General Data Protection Regulation, U.S. universities and colleges are recommended to evaluate whether they will need to comply with the new privacy regulation.