Compliance Alert

Brought to you by: Ethics, Compliance and Audit Services

Audit Compliance Investigations Presidential Policies Contact

UNIVERSITY OF CALIFORNIA

This Issue's Contents

Audit and Investigations

Making Credibility Determinations in Workplace Investigations

Who doesn't like a good criminal investigation television drama? From the various spin-offs of *Law and Order* to *CSI: Crime Scene Investigation*, the actors portrayed in these shows make investigations look easy and exhilarating. Unfortunately, workplace investigations usually are not the same as in these crime dramas. However, they can involve similarly challenging issues that require the skills of a trained investigator and not a paid actor. Conducting workplace investigations can seem easy enough: receive a complaint, gather evidence, conduct interviews, and determine whether a policy or law was violated. Nonetheless, trained workplace investigators know that this is not the case. For instance, in investigations where you have a "word against word" or "he said/she said" situation, an investigator cannot simply take the evidence provided to make a decision. Rather, this requires a trained investigator to make credibility determinations of the parties and witnesses to determine the accuracy of their statements. Thus, it is an investigator's responsibility to make reasoned credibility assessments in order to make factual findings.

To begin with, before starting any investigation an investigator needs to recognize and eliminate their own "unconscious biases." "Unconscious biases" are hidden predispositions that can take the form of assumptions we make about people or events, as well as the subsequent actions we take, without recognizing the reasons behind them. Note that a common tactic for discrediting a workplace investigation is to attack the investigator's perceived impartiality. Recognizing and eliminating our own "unconscious

Here's What's Happening at ECAS

- The search for a new Senior Vice President and Chief Compliance and Audit Officer (SVP-CCAO) has begun. The SVP-CCAO will guide the University of California's Ethics and Compliance Program, recently reaffirmed by the UC Regents. Further information forthcoming.
- ECAS is currently in the process of recruiting for the position of Director of Healthcare Compliance and is pleased to announce the position of Director for Research Compliance as open for interested candidates. Further information is available through the following link: UCOP Job Details.
- 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)
- Ethics and Compliance Training
  - The Compliance and Conflict of Interest for Researchers Briefing (COIR) course was rolled out to campuses in January 2017.
  - General Ethics and Compliance Briefing online course update to be rolled out in the Spring.
- Sexual Violence and Sexual Assault Education and Training Updates:
  - Online training module for staff and faculty will be translated into three languages: Spanish, Mandarin, and Tagalog. Estimated roll out date is Spring 2017.
  - UC's policy on Sexual Violence and Sexual Harassment is now available in Spanish and Mandarin translations.

biases," as investigators, is crucial for conducting fair and impartial investigations.

Next, in determining the credibility of witnesses and/or parties to the investigation, there are a number of factors that an investigator should consider:

1. **Source of information**
   - Was the witness at the event able to observe or hear it firsthand?
   - Did the witness rely on statements from others?
2. **Corroborating/Conflicting Statements**
   - Are there witnesses or documents that support or contradict one party's statement over the other? If there are contradictions, how important are they in the matter?
   - Does the witness support one account of events over another?
3. **Detail/Omissions**
   - How general or specific was a witness's statement and were any details supported by evidence?
   - Is there evidence to support the allegations?
4. **Inherent Plausibility**
   - Does the statement make sense?
   - Does one party's version of events challenge reasoning or common sense?
5. **Motive**
   - Does a party have a motive to lie about, exaggerate, or disagree with the incident?
   - Is there any history between the witnesses and/or parties that could influence the offered account?
6. **Prior Behavior**
   - Is there any evidence of similar behavior or other incidents between the parties?
   - Does the party's behavior on social media suggest a pattern?

No single factor is determinative. An investigator must evaluate the totality of the circumstances when assessing credibility. Careful consideration of the factors above can help an investigator resolve conflicting statements and make reasoned determinations. Also, understand that an investigator is not necessarily making a determination on whether a party or witness is lying. Rather, an investigator is determining how credible they find an account, based on the evidence provided.

—Michael Sandulak, ECAS

Cybersecurity

Cyber-Risk Coordination Center

As part of an ongoing effort to promote awareness in the area of cyber and information security, the Compliance Alert newsletter will periodically include cybersecurity articles, information and tips. In this issue, we introduce you to the Cyber-Risk Coordination Center, aka C3, which was created over the past year to act as a resource and support for systemwide cyber-risk activities. Reporting to the office of the UC systemwide Chief Information Security Officer, David Rusting, the C3 is currently comprised of:

- Monte Ratzlaff, Cyber-Risk Program Director
- Rebecca Nguyen, Cyber-Risk Technical Project Manager
- Julie Goldstein, IT Security Analyst
- Kamika Hughes, IT Security Analyst
- Jackie Porter, Cyber-Risk Technical Project Management Coordinator

Some of the projects the C3 has been working on include RFPs for breach response and forensic services, FireEye threat detection and identification (TDI) for all UC locations, coordinating and hosting semiannual Cyber Security Summits, and a systemwide NIST cyber security frame-work assessment. The staff also coordinated the promotion of National Cyber Security Awareness Month last October in conjunction with several campus locations: http://ucal.us/ncsam.

Because cyber and information security must be an ongoing practice, not just highlighted for one month a year or via a single annual training, the intercampus group that developed content for Cyber Security Awareness Month will continue to provide information and resources in this area. Examples are expected to include strategies for reaching various audiences (researchers, faculty, staff, students), promotion of good cybersecurity habits, poster templates, and other ways to foster a culture of information security awareness. As an example, C3 is now promoting information security awareness at UCOP's monthly new employee orientation.

We look forward to providing more cyber/information security content to you through the Compliance Alert newsletter in the future. Until next time, here are some important information security tips:

Focus on a few good cybersecurity habits instead of trying to remember many different dos and don'ts and best practices. The following good habits can help protect you in a variety of different situations:

1. Always think twice before clicking on a link or opening an attachment.
2. Verify requests for private information (yours or other people's), even if they look like they're from someone you know.
3. Protect your passwords.
4. Back up critical files.
5. If it's suspicious, report it!
6. Secure your area and computer before leaving them unattended – even just for a second. Take your phone and other portable items with you or lock them up.
7. Delete sensitive information when you are done with it.

If you would like more information about C3's efforts, please visit http://security.ucop.edu.

Protect Yourself from Tax Fraud

The new tax season for 2016 has begun. During this time, many scammers attempt to gain personal information from W-2 Wage and Tax Statements through phishing and malicious software (malware). Last year, some scams were directly aimed at UC employees. Some useful tips are offered to help UC employees better protect their sensitive information and that of others.

Ransomware Rising: Putting Our Files at Risk

Ransomware has grown in use by cybercriminals to gain unauthorized access to a user's computer system. This type of malicious software encrypts a victim's files, denying them access to their own documents. Cybercriminals then demand a ransom for restoring access to the user. Since its introduction approximately six years ago, this type of malicious software is a continued risk as cybercriminals continually expose vulnerabilities.

General Compliance

SEC Finds Violation for Failure to Require Code of Conduct Compliance

The Securities and Exchange Commission (SEC) found United Airlines had violated the Securities Exchange Act when it was discovered to have inadequate internal controls to enforce the company's Code of Business Conduct. As a result of an investigation, the SEC fined the company $2.4 million when it failed to enforce the anti-kickback and anti-bribery provisions in its policy that their CEO had violated. In an agreement with the Department of Justice, United Airlines has agreed to revise its policies and procedures and improve its Ethics and Compliance Office.

Health Sciences Compliance

$5.5 Million HIPAA Settlement Shines Light on the Importance of Audit Controls

The Memorial Healthcare System (MHS) was fined $5.5 million by the Department of Health and Human Services (HHS) for potential violations of the HIPAA Privacy and Security Rules. Despite having policies and procedures in place for information access, MHS reported 115,143 protected health information records were accessible to unauthorized employees and affiliated staff. As such, HHS found MHS failed to properly review user access regularly.

Lack of Timely Action Risks Security and Costs Money

The Children's Medical Center of Dallas failed to request a hearing with the Office for Civil Rights once it had received a Notice of Proposed Determination. The Children's Medical Center was found to have failed to implement its risk management plan and did not provide encrypted device alternatives. As a result, the medical center would have to pay the full penalty of $3.2 million.

Human Resources Compliance

Education Department Releases Latest List of Title IX Investigations, After Failing to Do So

Since 2014, the U.S. Department of Education has made available a public list with the names of universities undergoing Title IX investigations conducted by the Office for Civil Rights (OCR). After an initial delay, the first updated list under the Trump administration was released to the public and news outlets. Currently, there are approximately 306 open cases spanning over 225 universities in the United States.

Research Compliance

Notice of the Publication of the Final Rule on the Federal Policy for the Protections of Human Subjects

The Department of Health and Human Services and 15 other federal agencies recently updated the final rule, also known as the Common Rule or the Federal Policy for the Protection of Human Subjects, in order to enhance the protections for human subjects participating in research.

Additional Resources:

1. Federal Policy for the Protection of Human Subjects
2. Notice of Clarification on the Final Rule

Update on Clinical Trial Funding Opportunity Announcement Policy

The new policy requiring all applications involving one or more clinical trials be submitted through a Funding Opportunity Announcement has a new effective date of January 25, 2018.

Notice of Extension of Effective Date for Final NIH Policy Requiring the use of a Single IRB for Multi-site Research

The National Institutes of Health (NIH) issued a new policy requiring all multi-site studies involving the same protocol to use a single IRB. Recently, the NIH has extended the effective date of this policy to September 25, 2017.

US Revises Russia Sanctions for Electronics Exports

Sanctions imposed on Russia's Federal Security Service (FSB) by the Department of the Treasury's Office of Foreign Assets Controls (OFAC) prohibited U.S. companies from requesting approval for importing encrypted devices into Russia. This included submitting notifications to the FSB for traveling with encrypted electronics (such as mobile phones and laptops). However, a recent OFAC publication revises these sanctions.

Additional Resources:

Publication of Cyber-related General License

Policy

Recent UC Policy Updates

Payroll: Official Pay Dates:

As of 12/31/2016, this policy was reformatted to a new template. Minor technical corrections were made to reflect current terminology, remove references to semi-monthly and monthly arrears pay cycles, and removal of Appendixes I-V.

PPSM 21: Selection and Appointment:

Policy changes effective as of January 27, 2017:

- Added language to require a criminal history background check on the final candidate recommended for hire in a critical position.
- Expanded language on how to review and assess background checks.
- Added a new section on reference checks.
- Clarified language and updated critical positions chart.
- Rescindment of the *Personnel Policies for Staff Members 21 (Appointment)* policy dated 10/1/2012.

Privacy

Email Lists Revealing Students' Private Information Remained Public for Years

Upon notification from Harvard University's newspaper, The Harvard Crimson, the Harvard Computer Society became aware that some of their student managed email lists were public and revealed private information. Email lists with public status would archive messages containing sensitive information such as: students' grades, financial aid information, and a social security number. These messages remained publicly viewable and could be in violation of a federal law, the Family Educational Rights and Privacy Act (FERPA).

Upcoming Educational Opportunities

- April 6—The Need for Robust HIPAA Security Risk Analysis Processes (Webinar)
- April 12-13—UC Healthcare Audit Training (UCLA)
- TBA—2018 Compliance and Audit Symposium