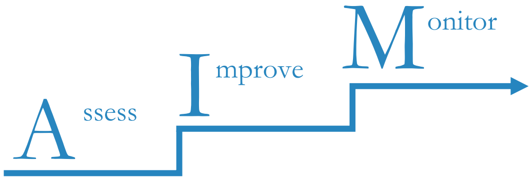
UCSF Medical Center at Mount Zion
UCSF Medical Center | UCSF Benioff Children's Hospital

AUDIT AND ADVISORY SERVICES



AIM higher

SYSTEM ACCESS AND YOU

AAS performs multiple system reviews every year, and one of the most common issues seen is insufficient system access controls. Below are some actions you can do to improve system access security and help protect UCSF informational resources.

1. Employee Separation: Disable Accounts

What is required:
UC policy requires access to be revoked upon termination, or when job duties no longer require a legitimate business reason for access. It is the departmental managers' responsibility to ensure all accounts created for separated employees are disabled.

What to do:

- Disable accounts in departmental systems
- Notify system owners of separation for non-departmental systems
- Perform periodic reviews to ensure that there are no active accounts belonging to separated employees in your department.

Why:
If accounts are left active, they may be used for unauthorized access that isn't able to be quickly detected.

(*cont'd on page 2)*

INSIDE THIS ISSUE

Fraud corner 2
Data analytics 3

SPECIAL POINTS OF INTEREST—JULY 2015 DATA BREACHES

- UCLA —potentially 4.5 million people affected by cyberattack
- Montefiore Health System—PHI theft ring stole information on more than 12,000 patients
- Harvard University—data system intrusion by hackers, unknown data access
- Siouxland Anesthesiology Pain Clinic—foreign hacker may have obtained PHI from over 13,000 patients
- University of Connecticut—Engineering school servers compromised by Chinese hackers, at least 1,800 accounts accessed

FRAUD CORNER

Protecting health data to prevent medical identity theft

With over two million people victims of identity theft each year and increased number of data breaches, medical identity theft is a growing problem. The "Denver Post" on 6/5/15 reported that a woman in Colorado accused of using false identity to receive nearly $500,000 in discounted medical care (reported in "*The Denver Post*" dated 6/5/15).

So what can we do to prevent and detect medical identity theft? UCSF Medical Center's "Identity Theft Prevention, Detection and Response" Policy 1.02.21 (**http://manuals.ucsfmedicalcenter.org/AdminManual/IndividualPolicies/IdentityTheftRedFlag.pdf**) gives a great list of things to check, but in general, being aware and alert for things that seem out of place, patients requesting name changes to their health record, checking and verifying IDs and patient information will help identify victims and perpetrators of medical identity theft, and minimize the risk to our patients and our organization.

If you have any questions or concerns about fraud, you can contact Audit and Advisory Services at (415) 476-3851, or call the whistleblower hotline at 1-800-403-4744 or via the Ethics Point website.

SYSTEM ACCESS AND YOU (CONT'D)

2. Shared Accounts: Create Individual Accounts

What is required:

UC policy states that passwords to individual accounts should not be shared with other individuals.

What to do:

- Learn about risks for sharing files or sharing identity.
- Create individual accounts.
- Request an exception approval if it is not feasible to create individual accounts.

Why:

If employees share accounts, it may be difficult to assign culpability if the account is used improperly.

3. Password: Use Strong Passwords

What is required:

UCSF Password Standard defines minimum password requirements.

What to do:

- Use a strong and hard-to-guess password
- Avoid reusing passwords or using the same password everywhere
- Don't enter your password on untrusted systems
- Remember to change your passwords on a periodic basis

Why:

More complex passwords are harder for hackers to guess. If the same password is used everywhere, it is like carrying one key that unlocks your house, your car, your office, your briefcase, and your safety deposit box – once one account is compromised, they all are.

4. Session Timeout: "Lock" devices

What is required:

UC policy requires devices that access restricted and/or essential services that are left unattended for an extended period of time shall employ measures, such as session timeout or lockout mechanisms, that require re-authentication before users return to interactive use. UCSF policy requires devices to be configured to "lock" and require a user to re-authenticate if left unattended for more than 20 minutes.

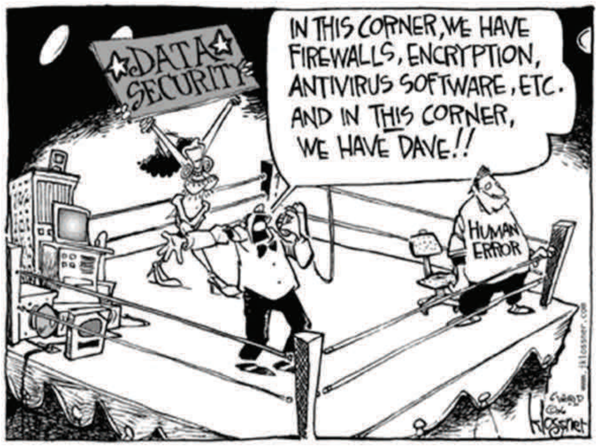
What to do:

- Configure to "lock" devices left unattended for an extended period of time
- "Lock" your workstation (Ctrl-Alt-Delete) before you walk away from it

Why:

If devices aren't locked, someone may be able to use your account without your knowing.

With the increasing frequency of cyber attacks, managing system access is one way to help strengthen information security. Keeping UCSF's information protected requires participation from everyone at UCSF.


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

Computerworld cartoons by John Klossner

DATA ANALYTICS

Continuous Analytics Programs

The purpose of a Continuous Analytics Program (CAP) is to enable business management to continually review business processes for adherence to and deviations from their intended level of performance and effectiveness. A good CAP can assist management in assessing the effectiveness of internal controls, detecting compliance risks, improving business process activities, and executing more timely quantitative and qualitative risk related decisions. Due to the automated and continuous nature of CAPs, an organization is able to monitor controls in a more cost effective manner.

Strong CAPs are an asset to any organization as environments become even more complex and the volume of data generated by the organization continues to increase.

1855 Folsom Street
Suite 107
San Francisco, CA 94143
Phone: (415) 476-3851

AuditAdvisor@ucsf.edu
http://audit.ucsf.edu

UC Whistleblower website and Hotline:
http://ucwhistleblower.ucop.edu
(800) 403-4744

CONTINUOUS ANALYTICS AT UCSF

Audit and Advisory Services (AAS) has developed a framework for implementing a robust Continuous Analytics Program (CAP) here at UCSF. As a part of AAS's efforts to provide internal clients with a tool that provides increased confidence, impact, insight, and root cause analysis abilities, AAS has invested in ACL Desktop and ACL Analytics Exchange to develop ad-hoc analysis, customizable scripts, and reports that can be used by internal client partners.

AAS partners with departments to assess their needs and develop customizable scripts that can be implemented into the department's business processes. One example of this synergistic process was the development of the P-Card scripts to monitor for fraudulent purchases within Supply Chain Management. In addition, to providing data analysis and CAP services, AAS also provides training on ACL Scripting to internal client partners and other audit teams.

As the CAP continues to mature at UCSF, AAS will increase collaboration with counterparts at other UC campuses in order to expand on current capabilities and provide more robust reporting and visualization abilities.

SPOTLIGHT ON OUR TEAM

When the initial idea for an Audit and Advisory Services (AAS) team building activity was proposed, there were creative ideas coming from all corners. As we looked at the options from all aspects; however, the one that stood out as really identifying with what our goals are for AAS within UCSF was helping at the SF Marin Food Bank. From efficient use of resources to education and support, the SF Marin Food Bank provides a full spectrum of services to the community, and was the clear choice for us to take a step back from our everyday work and see how we all can work together to provide support to a wider population.

Our activity was a great success – we worked efficiently together and surpassed the goals for food sorting and packaging.

Pictured from left to right:
Back Row: Paul Lapachet, Randy Otsuki, Trenicia Williams, Susan Walker, Josephyne Quach, Mike Lee
Front Row: Tom Poon, Sugako Amasaki, Irene McGlynn, Zuleikha, Shakoor, Adriena Groves-Harris
Not Pictured: Mark Mayeda

ASK YOUR AUDIT ADVISOR

Are there any questions you have been wondering about related to audit, risk, controls, or advisory services? Are you curious about what the audit process entails, how areas get selected for audits, what exactly is an advisory project, or what risks you need to consider when doing a system implementation? Our "Ask Your Audit Advisor" corner will be featured in every issue of the newsletter. Send us your burning questions and we will answer them here! You can also ask questions through the AAS e-mail AuditAdvisor@ucsf.edu