

The Role of the CMIO in Advancing Cybersecurity

AMDIS 2017

Brian Clay, MD

Chief Medical Information Officer, Inpatient and Hospital Affiliations

UC San Diego Health

Disclosures

- None

University of California, San Diego Health



University of California, San Diego Health Overview

- **Our Mission:** To deliver outstanding patient care through commitment to the community, groundbreaking research and inspired teaching.
- **Our Vision:** To create a healthier world — one life at a time — through new science, new medicine and new cures.

FY 2015 Key Statistics

- Number of Employees: 7,500+
- Annual Discharges: 28,043
- Average Daily Census: 451
- Emergency Visits: 74,280
- Total Outpatient Visits: 636,118
- Average Length of Stay: 5.9 days

UC San Diego Medical Center: UC San Diego Medical Center, Thornton, Sulpizio, Jacobs
combined bed capacity 808 beds

UC San Diego Academic Enterprise: School of Medicine, Pharmacy
Faculty: 1,431; Students: 2,370
Research Awards (FY 2015) \$577 million








**KEEP
CALM
the
CMIO
IS HERE**

UC San Diego Health – Cybersecurity Roadmap

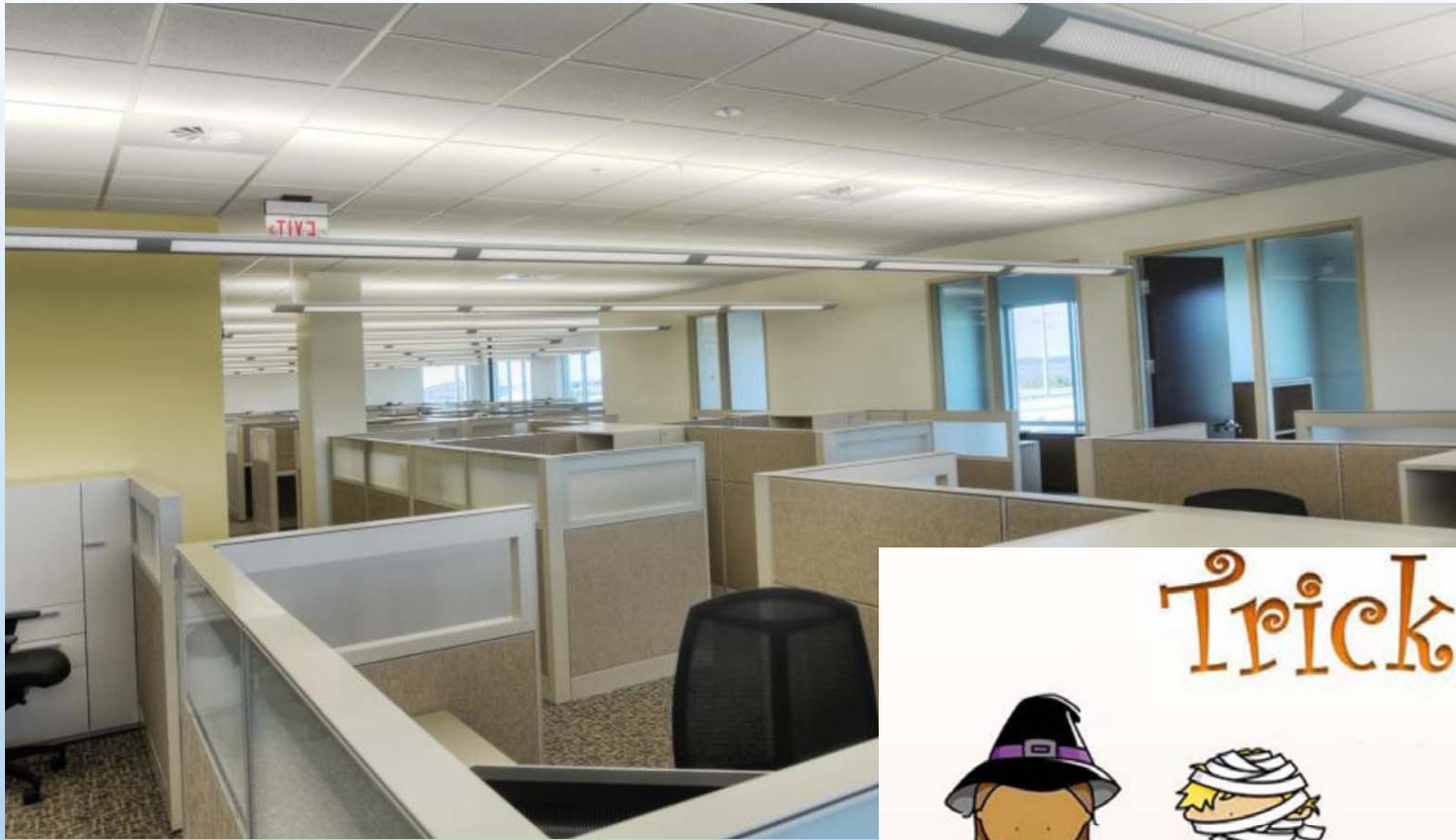
Completed projects

- Automated workstation timeout
- Secure email
- Two-factor authentication for remote access

Upcoming Projects

- Data loss prevention (DLP) scanning
- Secure messaging for mobile devices
- Removing local admin rights from workstations





Trick or Treat



Automated workstation timeout

- Workstations without automated timeout
 - Files with PHI left on desktop
- Configured all non-clinical workstations to automatically lock out at 20 minutes
 - Thousands of workstations
 - Included physician office workstations
- Grumbling from some docs – citing “inconvenience” of change

CMIO Job #1



CMIO Job #1 - Communication

- CMIO is often “the face of IT” for the medical staff
- Leverage your relationships with key physician leaders
 - Reach out to your supporters ***and*** your critics
- Get out there face-to-face with the docs! Emails by themselves are insufficient...
- Create a “road show”

UC San Diego Health – Cybersecurity Roadmap

Completed projects

- Automated workstation timeout
- Secure email
- Two-factor authentication for remote access
- **Mobile device management**

Upcoming Projects

- Data loss prevention (DLP) scanning
- Secure messaging for mobile devices
- Removing local admin rights from workstations

Mobile device management

- Many users using personal smartphones to access email, EHR mobile platform, etc.
- Desire to roll out MDM solution for personal smartphones
- Great communication efforts
 - Standard road show / talking points
 - Multiple physician meeting presentations

CMIO Job #2



KNOW YOUR CISO

CMIO Job #2 – Know Your CISO

- Mobile device management road show
 - Co-presented by CMIO and CISO
- As the CMIO, you know the clinical workflows, but maybe not all of the nuances of the security technology itself
 - Your CISO can help get those questions from physicians answered
 - Helpful to dispel misconceptions about the technology
- As the CMIO, you can influence the configuration of the security technology to best balance security and user experience

Secure email deployment



- Many users including PHI in email, and sending to non UCSD email domains
- Some users have their UCSD emails forwarded to non UCSD email domains
- Need to encrypt PHI-containing emails going outside UCSD

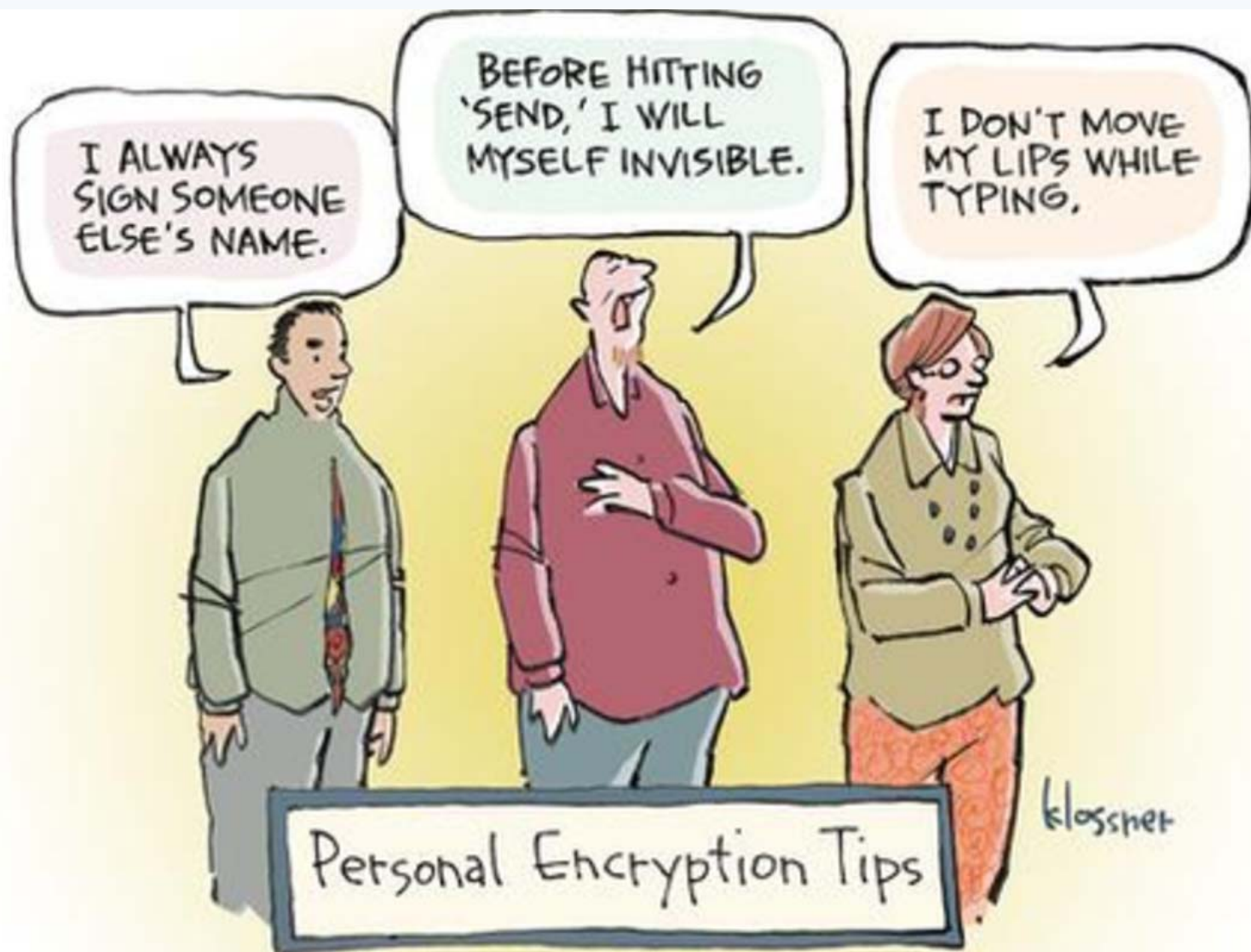
I ALWAYS
SIGN SOMEONE
ELSE'S NAME.

BEFORE HITTING
'SEND,' I WILL
MYSELF INVISIBLE.

I DON'T MOVE
MY LIPS WHILE
TYPING.

Personal Encryption Tips

klossner



CMIO Job #3




Secure email

- Add “Secure:” to subject line of email with protected information
- Encrypts email if sent outside the UCSD email domain

Secure email

- Sometimes demonstrating is far more powerful than explaining

 Send	To...	<u>Clay, Brian</u>
	Cc...	
	Subject	Question About This Patient

I wanted to ask you about Mr. Fake Q. Patient, MRN 1234ABCD...

Secure email

- Sometimes demonstrating is far more powerful than explaining

Send	
Subject	Secure: RE: Question About This Patient
Securing this email thread given presence of PHI.	
In regard to this patient...	
Brian Clay, MD	
Chief Medical Information Officer, Inpatient and Hospital Affiliations	
UC San Diego Health	

Secure email

- Sometimes demonstrating is far more powerful than explaining

Send	
Subject	Secure: RE: Question About This Patient
Securing this email thread given presence of PHI.	
In regard to this patient...	
Brian Clay, MD	
Chief Medical Information Officer, Inpatient and Hospital Affiliations	
UC San Diego Health	

Secure email

- Well adopted throughout enterprise
- Users now more comfortable sending PHI via email if needed
- Also took opportunity to re-educate users on policy of sending PHI via email (allowed, but minimum necessary)

Two-factor authentication for remote access

- Users could access EHR and other clinical systems remotely with just standard AD credentials
- Did “security questions”, but not true two-factor process
- Successfully deployed 2FA for electronic controlled substances prescribing using smartphone application
- Next step: 2FA for all remote access to clinical systems

2FA - Challenge

- EPCS 2FA – provider opt-in
- Remote access 2FA -- requirement

2FA - Challenge

- EPCS 2FA – provider opt-in
- Remote access 2FA – requirement
 - Providers concerned about efficiency and use of personal smartphones as 2nd factor



2FA – Communication / Preparation / Testing

From: medstaff <medstaff@ucsd.edu>

Date: May 30, 2017 at 8:13:58 AM PDT

Subject: Coming in June 2017: Two-Factor Authentication Roll-Out for Remote Access to the Clinical Web Portal (CWP)

PLEASE NOTE: The MedStaff e-mail is used for informational e-mails only. Please do not reply back as it is not continually monitored.

This message is sent on behalf of Dr. Christopher Longhurst, Chief Information Officer and Clinical Professor; Dr. Brian Clay, Chief Medical Information Officer, Inpatient and Hospital Affiliations, and Dr. Marlene Millen, Chief Medical Information Officer, Ambulatory.

This is a follow-up communication to the CIO message sent to UC San Diego Health on May 4, 2017. **If you use Epic from home or offsite, please read to avoid delays when logging in to the Clinical Web Portal.**

Two-factor authentication for remote access

- Deployed in early June 2017
- Successful go-live, no big issues
- Provider feedback indicates that 2FA not disruptive

2FA – Some (Non-Representative) Provider Feedback

“As a triple-board certified physician I appreciate the importance of patient privacy and HIPAA issues, and am all in favor of a systematic and strong response to current cybersecurity threats. But what is needed is a coordinated, cooperative, collegial approach to the problem, something I have not seen so far.

I have never seen anything quite like the current aggressive unilateral action against the faculty in the implementation of these cybersecurity efforts.

You should know that many faculty are now worried about a “big Brother is watching” scenario, and have warned me about speaking out, because I might run the risk of being selectively targeted for attention by IT.”

-- Faculty physician at UC San Diego Health

CMIO Job #4



HAVE A THICK SKIN



CMIOs and Cybersecurity

- You have a role to play!
- Communication
- Partner with your CISO
- Lead by example
- Welcome feedback and criticism

Questions?

Brian Clay, MD

bclay@ucsd.edu

@brianclaymd