UW Medicine
Data Stewardship

Lenny Sanchez
UW Medicine Compliance

UW Medicine

AGENDA TOPICS

- Defining data stewardship and your responsibilities
- Safeguarding DOs
- Current security threats
- Tools and resources

What is Data Stewardship?

- **Every individual** is personally and professionally responsible for the security and integrity of the confidential information (electronic, paper or verbal) entrusted to you.

- **UW Medicine Professionalism Policy**: Demonstrated excellence, integrity, respect, compassion, accountability and a commitment to altruism in all our work interactions and responsibilities.

Data Types at UW / UW Medicine

What This Means

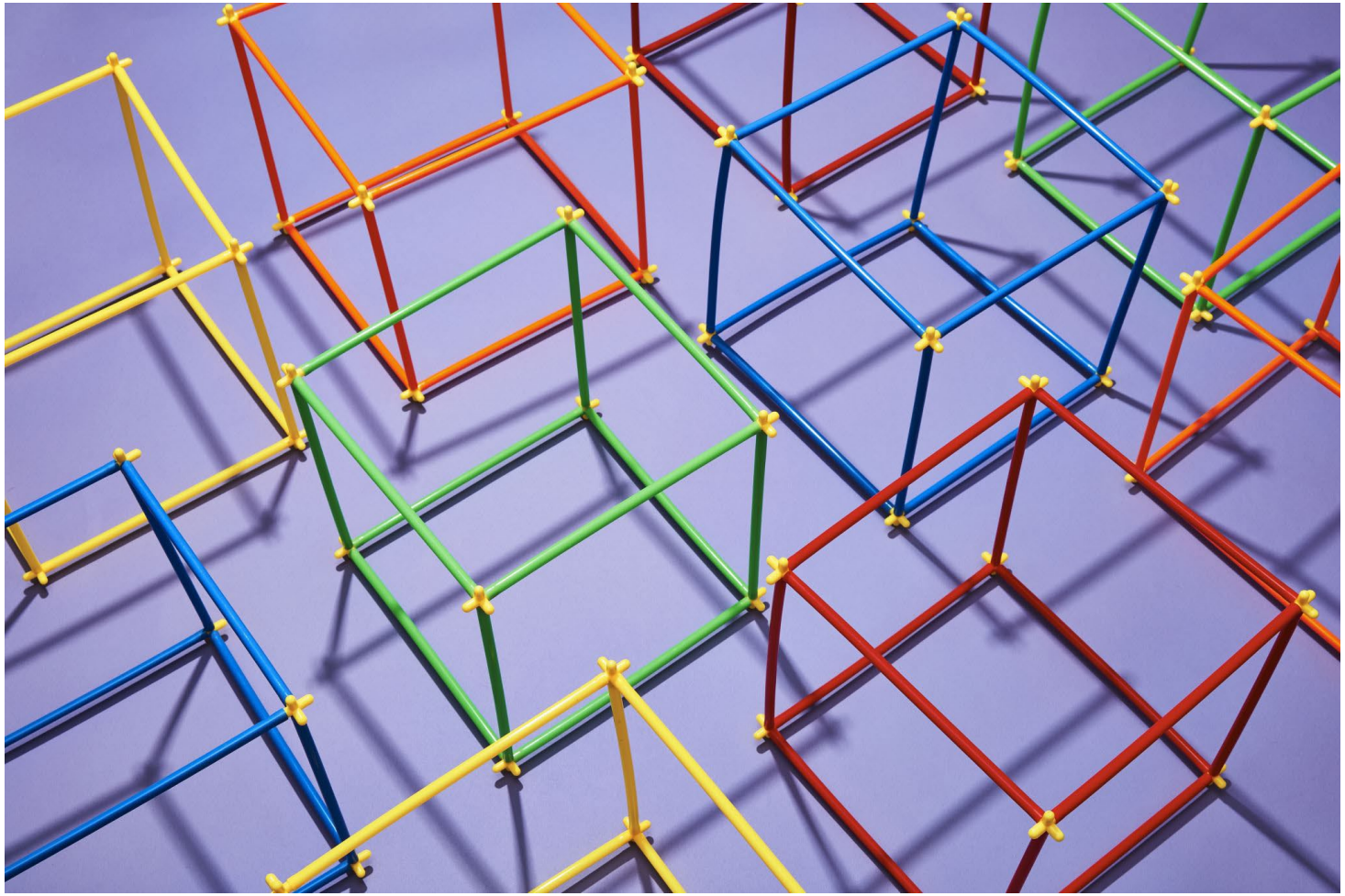
It is your personal, professional and ethical responsibility to protect the information used in the course of your work for UW Medicine, keeping it safe and secure and protecting it from loss and theft.

Safeguarding Confidential Information

General purpose of safeguarding information is to retain trust with patients and prevent “breaches”

Breaches may require notification to individuals, the media, and government regulators

Data Stewardship: DOs



Do #1: Encrypt Devices

Encrypt your mobile phone and laptop

Why? Lost or stolen data on an encrypted device generally does not result in a “breach” because it has been rendered unusable/unreadable

Do #2: Encrypt Emails

1. Use Microsoft O365/Outlook to conduct work related to the UW Medicine clinical enterprise (not Gmail/G Suite)
    - Emails are automatically encrypted when sent between @uw.edu accounts and our main partners (SCCA, Fred Hutch, Seattle Children's, etc.)

2. Attach an encrypted file and send the encryption password in a separate email

Do #3: Secure Destruction

Remove confidential data prior to disposing of your personal device or returning your assigned device to your IT Department

Be mindful about files containing confidential information saved on your local hard drive – move files to secure network drives or OneDrive for Business when appropriate

DO #4: Take confidential data out of your car

UW Medicine Compliance regularly receives reports of car thefts and stolen laptops/papers

Don’t let this happen to you!

Examples – PHI Incidents

Accessing medical records of friends/family/exes

- Most common patient/employee concern, but also receive reports from other healthcare facilities
- Recent situations: parent accessing child's record, child accessing parent's record, employee accessing record ex-significant other's record,
- Corrective action varies, but harshest occurs with presence of bad intent

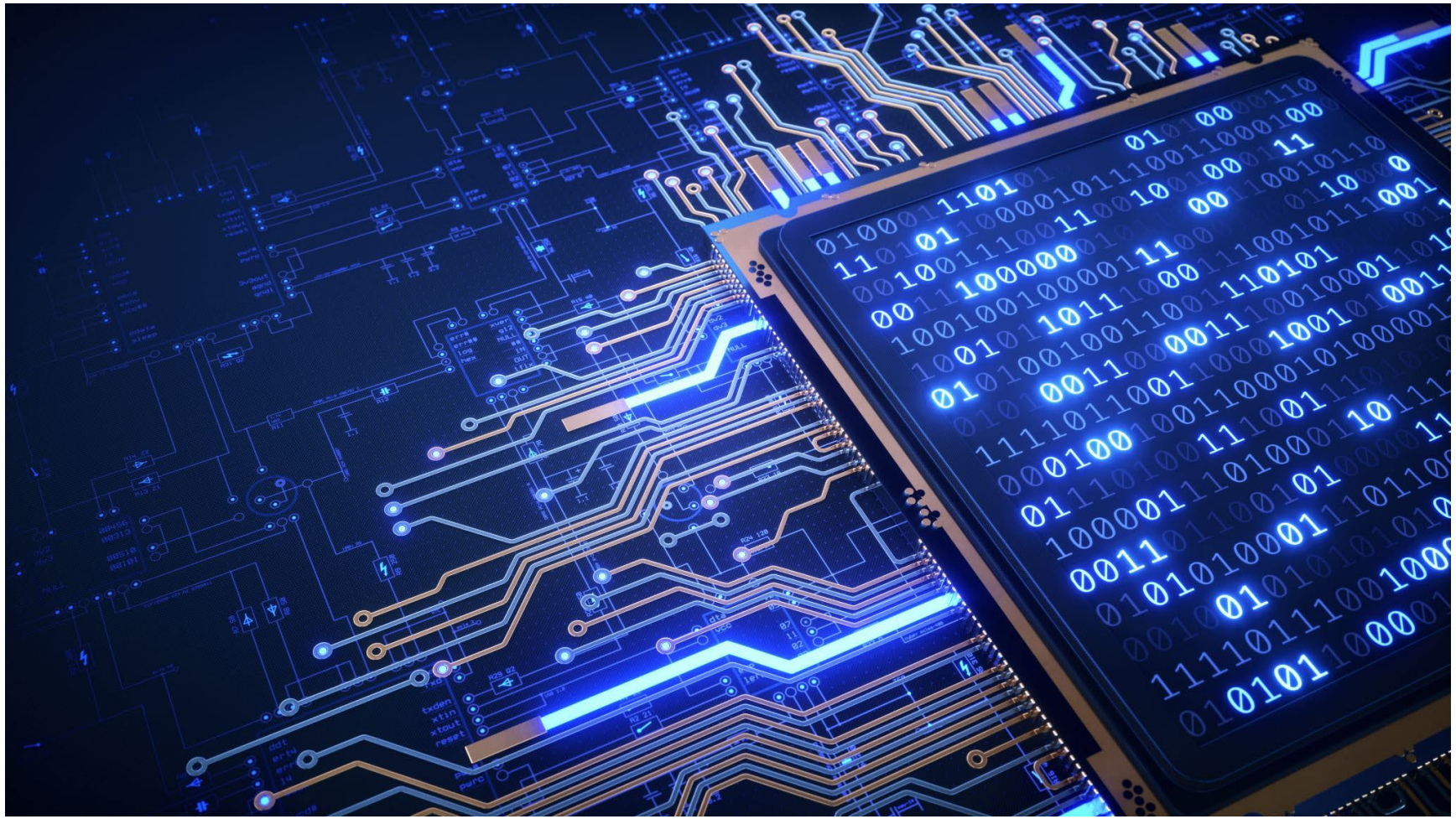
Leaving the medical record open

- Provider fails to lock computer screen when leaving patient room
- Patients concerned about privacy of patients on the screen; concern their info will be treated similarly

Emailing confidential data to wrong person; non-UW email address

- Be mindful of recipient email addresses, particularly if they're personal accounts (i.e., Gmail, Hotmail, etc.)

Security Threat: Phishing



Phishing

Designed to trick a person into giving up:

- Personal and professional credentials
- Account information
- Other identity information to access your personal or professional information and systems

Goal is to steal/sell confidential data; Ransomware

Phishing Example: Too good to be true?

PART-TIME JOB OFFER!!

College Central Network: Job Referral

Stilt Connection International Relief continues to help alleviate suffering during the COVID-19 crisis. We have launched new efforts or adapted projects to support people who are suffering during this global pandemic. We are looking for students and Locals for a paid , Short-term, temporary (Part-Time) position. It doesn't require any specialized skills and you can work from home with reasonable wages & bonuses.

JOB DESCRIPTION:

? Prepare and ship packages, educational materials, testing supplies, and appropriate forms to Volunteers.

? Answering phones and providing information about services and programs

? Wages (including miscellaneous): $400

Other Benefits inclusive:

Interested Candidates should contact us for more Information about the job opening through: [redacted]

[redacted]

Collection Center Coordinator

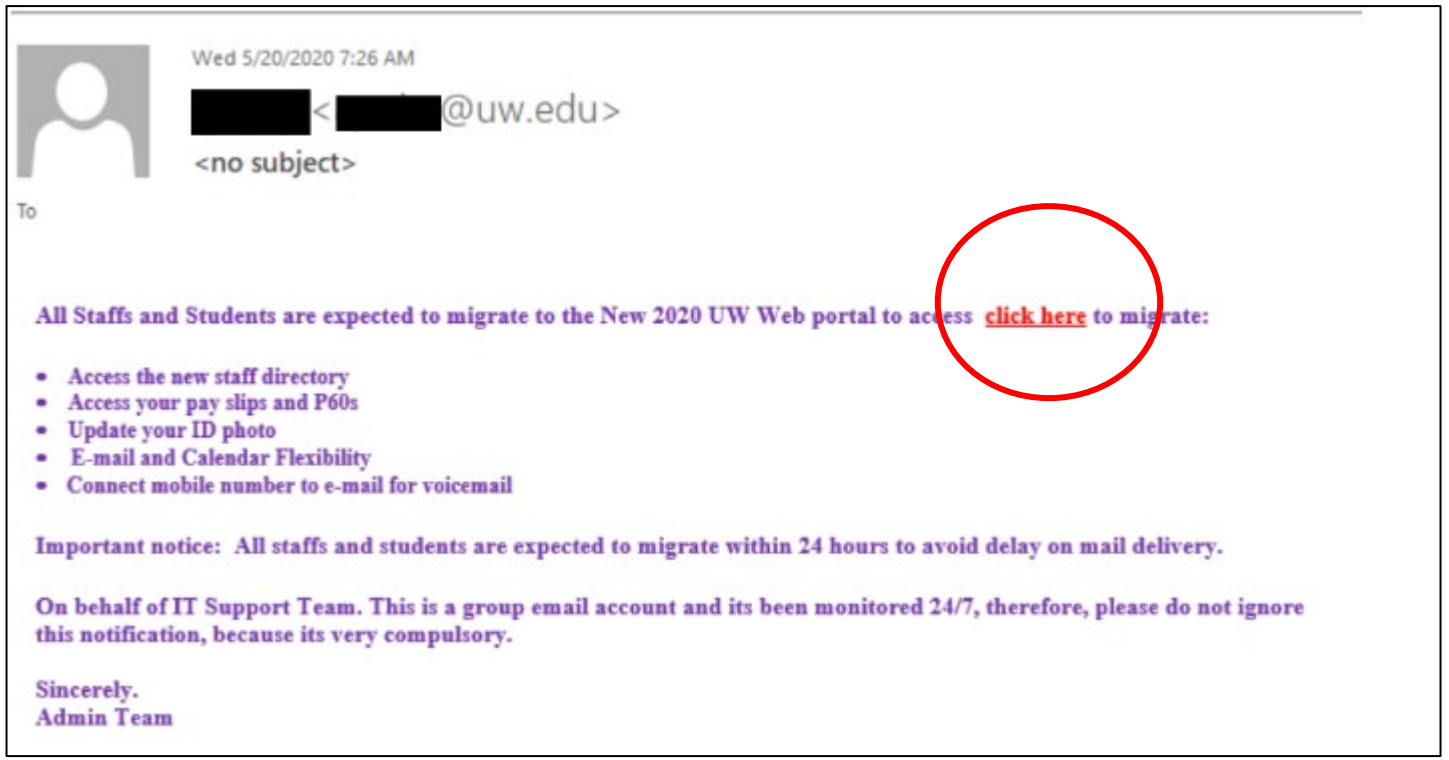
[redacted] International Relief

Phishing Example: Click the link

*Don’t click the link

*Hover over the email address and link

*Delete and/or report suspicious email



Wed 5/20/2020 7:26 AM

[redacted]<[redacted]@uw.edu>

<no subject>

To

All Staffs and Students are expected to migrate to the New 2020 UW Web portal to access click here to migrate:

- Access the new staff directory
- Access your pay slips and P60s
- Update your ID photo
- E-mail and Calendar Flexibility
- Connect mobile number to e-mail for voicemail

Important notice: All staffs and students are expected to migrate within 24 hours to avoid delay on mail delivery.

On behalf of IT Support Team. This is a group email account and its been monitored 24/7, therefore, please do not ignore this notification, because its very compulsory.

Sincerely.
Admin Team

Recent Ransomware Attack

- UWM vendor's employee unwittingly gave login credentials to bad actor
- Bad actor encrypts PHI; vendor pays ransom
- Vendor notifies all clients
- All clients, including UW Medicine, had to determine whether to:
    - Whether to notify patients
    - Notify media
    - Notify regulatory
- Regulatory investigation required when when breach affects >500 individuals

Thousands of patient records exposed after ransomware attack on CaptureRx

At least five healthcare providers were affected by the incident, which occurred in February.

By Kat Jercich | May 11, 2021 | 11:25 AM

Photo by Sora Shimazaki from Pexels

A ransomware attack on the healthcare administrative-service provider CaptureRx has exposed patient information from multiple provider systems.

Phishing: Bottom Line

- UW/UW Medicine will never ask for account information via email
- UW Medicine periodically sends phishing messages to our workforce to help raise awareness
- **YOU WILL RECEIVE PHISHING MESSAGES** – if you're unsure, send a separate email to the purported sender to verify they sent the email

TOOLS and RESOURCES

Tools to Assist You in Safeguarding Data

- Creating strong passwords

  https://depts.washington.edu/uwmedsec/restricted/accounts-and-passwords/
- How to encrypt

  https://depts.washington.edu/uwmedsec/restricted/guidance/encryption/
- Securing your physical space
  - Contact your building facilities department
- Education and training materials

  https://depts.washington.edu/uwmedsec/restricted/services/education-training-and-awareness/
- UW Medicine Privacy, Confidentiality and Information Security Agreement (PCISA): http://depts.washington.edu/comply/docs/002_F1.pdf

Cloud Resources

- OneDrive for Business

  https://itconnect.uw.edu/wares/online-storage/onedrive/

Phishing Resources

- UW Medicine IT Security Phishing and Spam Email Guidance: https://depts.washington.edu/uwmedsec/restricted/guidance/phishing-and-spam-email-guidance/

- Office of the Chief Information Security Officer phishing video: https://ciso.uw.edu/education/online-training/#phishing

Other Resources

- Office of the Chief Information Security Officer
  - http://ciso.washington.edu/
- UW Medicine IT Security
  - https://depts.washington.edu/uwmedsec/restricted/about-its-security/
- UW Medicine Professionalism Policy
  - https://www.uwmedicine.org/about/policy-on-professional-conduct

Contact Information

- Dean of Medicine IT: domhelp@uw.edu; 206.221.2459
- SoM Academic and Learning Technologies: somalt@uw.edu
- UW Medicine IT Services Help Desk: mcsos@u.washington.edu
- UW Medicine Compliance: comply@uw.edu; 206.543.3098
- UW-IT: help@uw.edu; 206.221.5000

Incident Reporting

- If you get infected, or think you may be infected, contact DOM IT at domhelp@uw.edu
- Report information security incidents when they occur to DOM IT
- Report the loss or theft of PHI to UW Medicine Compliance at 206.543.3098 or comply@uw.edu