UW MEDICINE WORKFORCE

PERSONAL ACCOUNTABILITY FOR DATA STEWARDSHIP

2013

UW Medicine

AGENDA

- Personal experience of a department chair
- Recap of Data Stewardship Education and Awareness Campaign over past year
- Results of campaign--what have we learned?
- Next steps

SUMMARY OF THE PROBLEM

- Incidents of loss or theft of patient information
- Considerable time and effort spent on investigation, review and any necessary responses and notifications
- Possible harm to individual and/or institutional reputation

SUMMARY OF EDUCATION AND AWARENESS CAMPAIGN

- 9/28/2012 Letter from Dean Ramsey
  - Personal and professional accountability for safeguarding confidential and patient information
  - Senior leadership and department, division or unit leaders responsible for ensuring that all individuals within their jurisdiction have encrypted and password-protected all devices used for work that contain confidential or patient information

SUMMARY OF EDUCATION AND AWARENESS CAMPAIGN

- Focused training and education program
  - Set and communicate clear expectations for all workforce members to safeguard confidential and patient information
  - Provide toolkit that included guidance for encryption, roles and responsibilities, PCISA form and educational materials to cascade communications throughout the system in a consistent manner
  - Widespread dissemination of information to faculty, residents, students and staff

RESULTS SO FAR

Since Dr. Ramsey's letter, there have been 15 losses or thefts of devices or equipment, including CPUs, laptops, flash drives, hard drives and phones

- 10 involved loss of patient information
  - 5 faculty, 3 residents, 1 medical center staff and 1 medical center department
  - 7 laptops, 2 flashdrives and 1 phone
  - 4 of the mobile devices were encrypted (3 laptops, and 1 phone)
  - 5 stolen from home, office or car and 5 lost

RESULTS SO FAR - CONTINUED

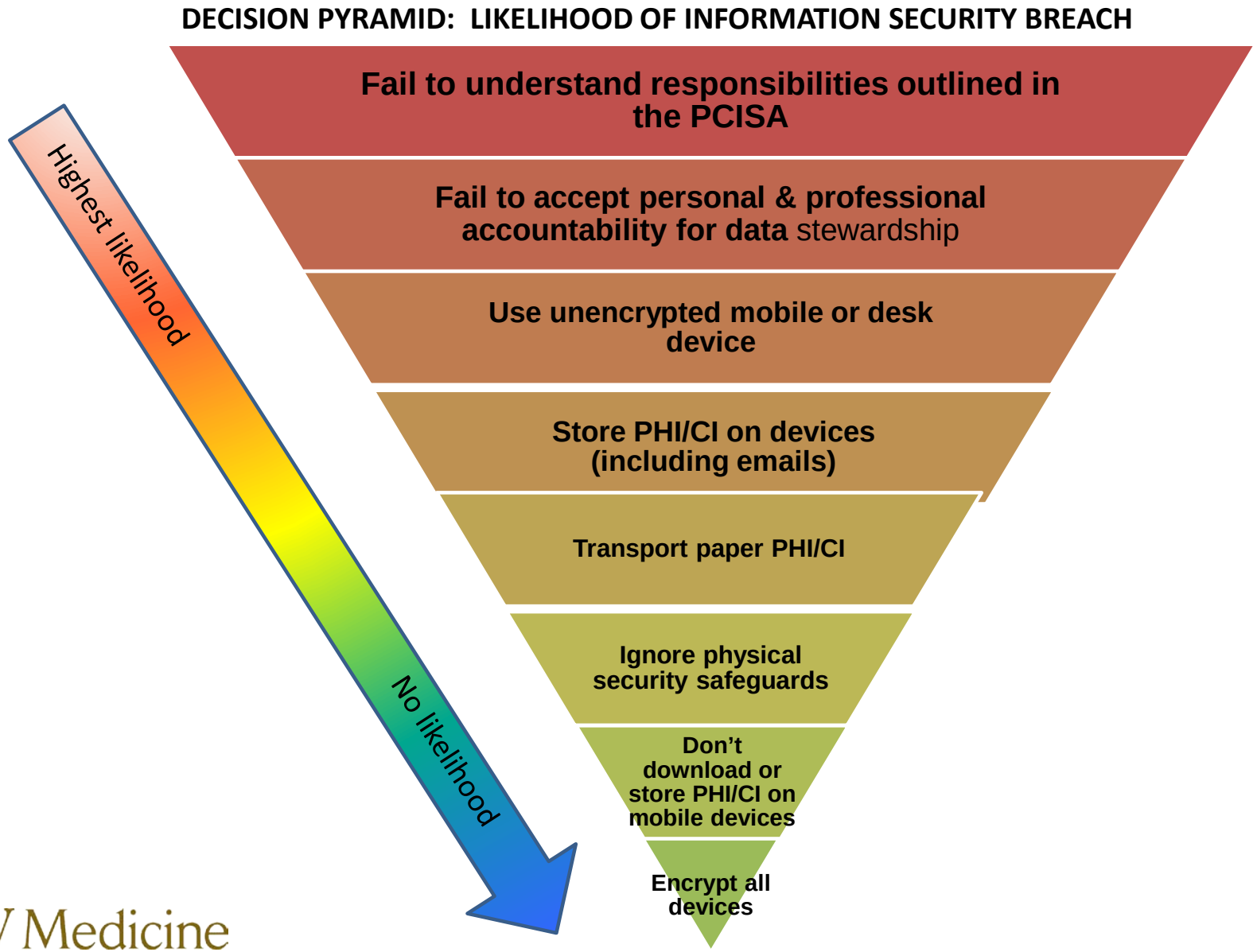
Previous time period – 14 total losses or thefts

- 6 involved loss of patient information
    - 2 faculty, 2 resident or fellow, 1 medical student, 1 medical staff
    - 4 laptops, 1 external hard drive and 2 involved hard copy loss
    - NONE encrypted, including 2 department-owned laptops
    - 5 stolen from home, office or car and 1 lost

WHAT HAVE WE LEARNED?

- More faculty and residents/fellows than staff (7/16 incidents involved faculty)
- Must assume devices will be stolen
- Most devices are not password protected or encrypted
- Physical security of information, including paper is important
- Majority of devices are UW-owned
- Message regarding personal accountability has been conveyed (“absolutely word has gone out”)
- However, the message has not been internalized by individuals

DECISION PYRAMID: LIKELIHOOD OF INFORMATION SECURITY BREACH



UW Medicine

WHAT WE WANT FROM YOU AS AN INDIVIDUAL

- Hold yourselves personally and professionally accountable
- You are responsible for the safekeeping of data in your possession
- Secure confidential information by encrypting and password protecting all devices, not taking the information off-site and double-locking away paper copies

WHAT WE WANT FROM YOU AS THE CHAIR

- Set the tone
- Reinforce the message
- Lead by example
- Ask for training and technical support
- Enable access to tools and resources for effective data stewardship
- Hold faculty and residents accountable

NEXT STEPS

Dean's Office

- Work with chairs to manage accountability
- Options include:
    - 25-71 process
    - merit review
    - incentive plan requirement
    - clinical privileges eligibility

NEXT STEPS

Compliance

- Develop a survey tool for self-certification
- Conduct random audits of School of Medicine departments

Questions ?

UW Medicine