OUCH! Newsletter – Staying Secure on the Road

This month's security focus is on *Staying Secure on the Road*. We know and understand most of you use the Internet while traveling, whether for personal or work related reasons. We want to be sure you can accomplish everything you need when on the road safely and securely. The OUCH! newsletter link is here http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201702_en.pdf

US DHHS Office of Civil Rights in Action – Lack of timely action risks security and costs money and $5.5 million HIPAA settlement shines light on the importance of audit controls.
The U.S. DHHS Office for Civil Rights (OCR) announced a civil penalty against Children's Medical Center of Dallas (Children's) of $3.2 million following the loss of an unencrypted, non-password protected BlackBerry device and the theft of an unencrypted laptop. The full article is here https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/childrens.
Memorial Healthcare Systems (MHS) has paid the U.S. DHHS $5.5 million to settle potential HIPAA violations because MHS failed to implement procedures with respect to reviewing, modifying and/or terminating users' right of access, as required by the HIPAA Rules. The full article is here https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/memorial/index.html.

Required Bi-Annual Access Control Auditing
As mentioned in the article above, HIPAA covered entities like the SoD are required to review and audit access to patient data systems and applications. To comply with that requirement all managers and supervisors need to go to https://www2.dentistry.unc.edu/secure/apps/ApplicationPortal/Validation/ and validate their employee's access to SoD systems and applications. Failure to complete this exposes the school to HIPAA penalties and fines.

Phishing
Please forward **as an attachment** any phishing messages that you encounter to phish@unc.edu.
For an explanation of how to forward an email as an attachment please read the following article on help.unc.edu.
To check and see if you have a suspected Phishing email go to http://its.unc.edu/phish-alerts/

Encryption Project Status
Encryption is one of the few technologies specifically mentioned in HIPAA. It is crucial to encrypt **ALL** mobile computing and mobile storage devices that could come into contact with patient data to comply with HIPAA and University policy. OCIS is now rechecking all 688 laptop for HIPAA compliance. You will be contacted by OCIS to bring your laptop down for a HIPAA spot check which takes about 20 minutes to complete. If you use USB Flash Drives with your encrypted laptop, they must also be encrypted and reported to OCIS. Failure to do so is a violation of HIPAA and University policy.
REMEMBER. If you have an unencrypted laptop or unencrypted USB Flash Drive and are using it here at the school, please contact OCIS as soon as possible! Don't get caught with an unencrypted device.

Backup Devices at your Home

It is always a good idea to have a backup of your data. OCIS has recently discovered that people are backing up patient data from their encrypted laptops onto home backup devices. Because of these recent events, you are prohibited from backing up patient data onto home backup storage **under any circumstances even if the backup device is encrypted.** If you have any patient data on your home backup device, remove it immediately. You should always store your patient data on secured University-managed, permanent storage which is automatically and securely backed up by the University. Contact OCIS to determine what secure permanent storage options are available to you or your program.

You can back up the non-patient data locations of your encrypted laptop's storage normally. If you have questions, please contact OCIS.

USB Hardware Encrypted USB Flash Drives Distribution

OCIS has received 649 hardware encrypted USB flash drives for certain programs, departments and staff. OCIS is currently distributing these drives to DDS, DH and Advanced Education.

SoD Security Awareness Training Test Requirement

To comply with HIPAA and UNC policy, OCIS is now enforcing the annual SoD Security Awareness Training requirement. To access the EPR, you will now be required to take and pass both the HIPAA and SoD Security Awareness test. To take the SoD Security Awareness Training and test please go to https://www.dentistry.unc.edu/secure/training/securityawareness/. OCIS recently updated the HIPAA and Security Awareness test to align with campus' content changes. If you have questions, please contact OCIS.

Cyber Security Awareness Posters Available

OCIS still has security posters that you can display in your department. Please come down to OCIS to pick up posters for your department or unit.

HIPAA Security Incident Update

The last reported HIPAA security incident was a lost, unencrypted USB flash drive. This incident is still under investigation.

We have gone seven days since the last HIPAA security incident. Stay vigilant.

OUCH! Archives

For previous issues and topics please go here:
https://securingthehuman.sans.org/ouch/archives

Security Awareness Tip of the Day

https://www.sans.org/tip_of_the_day.php

Remember. It is your personal responsibility to protect patient data (e.g. electronic Protected Health Information or ePHI) on laptop computers and portable media devices (e.g. CD/DVDs, USB keys, USB drives and SD Cards). In all cases, patient data can never be stored on a portable computing or media storage device unless it has been inventoried, encrypted and approved by OCIS.

Thanks and safe computing.

School of Dentistry HIPAA Security Officer
David Rankin
Email: david_rankin@unc.edu
Phone: (919) 537-3485

School of Dentistry HIPAA Privacy Officer
Dr. Darryn Weinstein
Email: darryn_weinstein@unc.edu
Phone: (919) 537-3588

School of Dentistry Compliance Specialist
Martin Folliard
Email: mfolliar@email.unc.edu
Phone: (919) 537-3444

For more information:
SoD Policies https://www.dentistry.unc.edu/experience/policies/
UNC Policies http://its.unc.edu/about-us/how-we-operate/
What is Sensitive Information? http://help.unc.edu/help/examples-of-sensitive-information/