

OUCH! Newsletter – Securely Using Mobile Apps

This month's security focus is on *Securely Using Mobile Apps*. We want people to make the most of their mobile devices safely and securely. The OUCH! newsletter link is here http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201703_en.pdf?utm_medium=Email&utm_source=Houselist+Ouch&utm_campaign=STH+Ouch!&utm_content=English+Version

US DHHS Office of Civil Rights in Action – Reporting and Monitoring Cyber Threats

The nation's health care system is part of the national infrastructure that has increasingly come under attack from cyber threats. One of the keys to combatting these cyber threats is for the government, the private sector, and international network defense communities to collaborate and share information. Covered entities and business associates should also monitor the US-CERT website for reports on vulnerabilities. Alternatively, information can be received directly via email by visiting US-CERT's Mailing Lists and Feeds. The full article is here <https://www.hhs.gov/sites/default/files/february-2017-ocr-cyber-awareness-newsletter.pdf>.

Required Bi-Annual Access Control Auditing

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. If you run into problems or think the information is incorrect, please contact Tim Murphy at Tim_Murphy@unc.edu.

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 laptops 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.

REMINDER - 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 personally owned backup devices. Neither the University nor the SoD give you permission to back up any patient data on

personally owned backup devices without written authorization. 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 students. To get your hardware-encrypted USB Drive, please go to the OCIS web link at <https://www.dentistry.unc.edu/secure/resources/usbkeys/index.cfm> follow the instructions and submit the on-line attestation. OCIS will verify your on-line attestation and deliver your hardware-encrypted USB Drive to your program's Admin or Business Manager. If you have any problems with the OCIS web link, please contact Tim Murphy at tim_murphy@unc.edu.

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 experienced a marked increase of finding unencrypted USB Flash Drives in meeting rooms and classrooms. Since we are a health care environment, we have to examine every flash drive we find for patient data and report any suspect data found to campus authorities. **Please use encrypted USB flash drives.** For information about encrypted flash drives, please contact OCIS.

We have gone 46 days since the last reported 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/>