OUCH! Newsletter – Passphrases
This month's security focus is on *Passphrases.* Passwords have traditionally been confusing, intimidating and overwhelming for most people. It is where security often fails because it is too hard. In this newsletter we explain passphrases, strong passwords that are easy to both remember and type. The OUCH! newsletter link is here
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_en.pdf

US DHHS Office of Civil Rights in Action – $2.5 million settlement shows that not understanding HIPAA requirements creates risk
In January 2012, CardioNet reported to the HHS Office for Civil Rights (OCR) that a company laptop was stolen from a parked vehicle outside of an employee's home. The laptop contained the ePHI of 1,391 individuals. OCR's investigation revealed that CardioNet had an insufficient risk analysis and risk management processes in place at the time of the theft. Additionally, CardioNet's HIPAA security policies and procedures were in draft form and had not been implemented. Additionally, CardioNet was unable to produce any final policies or procedures regarding the implementation of safeguards for ePHI, including those for mobile devices.
The full article is here https://www.hhs.gov/about/news/2017/04/24/2-5-million-settlement-shows-not-understanding-hipaa-requirements-creates-risk.html.

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
OCIS has received reports of Phishing attempt with the subject **"UNC.EDU HELP DESK."** If you see this email, DO NOT CLICK ON THE WEB LINK.
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. Starting Monday, May 1, OCIS will begin the process of rechecking all 688 laptops for HIPAA compliance. OCIS will send out a message to kick off this initiative. You will be asked to bring your laptop down for a HIPAA spot check that 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.

USB Hardware Encrypted USB Flash Drives Distribution
OCIS has received 649 hardware encrypted USB flash drives for certain programs, departments and staff. Starting Monday, May 1, OCIS will contact programs and departments that will receive these USB keys.

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 contact OCIS if you want a poster for your department or unit.

HIPAA Security Incident Update
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. **It has been 30 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 Deputy Security Officer
Nefertiti Holland
Email: nefertiti_holland@unc.edu
Phone: (919) 537-3485

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/