OUCH! Newsletter – Lessons from WannaCry
The security focus in the month of June is on *Lessons from WannaCry*. The recent breach has conveyed an important lesson towards how cybercriminals continuously improve and refine their methods and techniques of their attacks. Whether at home or at work, learn how to be prepared to take active steps to minimize impacts. The OUCH! newsletter link for the month of June is here https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201706_en.pdf

US DHHS Office of Civil Rights in Action – HHS Announces the availability of $195 million to expand substance abuse and mental health services at heath centers nationwide
In anticipation of September 2017, awards from the Department of Health and Human Services (DHHS) are expected to be made in the availability of $195 million to community health centers for expanding access to mental health and substance abuse services. DHHS's focus is on the treatment, prevention and awareness of opioid abuse. HHS has outlined five specific strategies to combat the ongoing opioid crisis. The full article is here https://www.hhs.gov/about/news/2017/06/26/hhs-announced-195-million-funding-to-expand-mental-health-and-substance-abuse-service-access.html

SoD Use of Microsoft 365 OneDrive
OCIS can now advise that OneDrive is available as **limited and conditional** use. Prior to using OneDrive with sensitive data, it is required to review, abide by and acknowledge the University's policies, guidelines and best practices regarding how to protect data in the cloud using OneDrive. Please go here to review : https://www.dentistry.unc.edu/secure/resources/onedrive/. Please complete the attestation form found at the end of the linked document. Informational sessions, security controls, and monitoring are forthcoming and will be announced. Please email OCIS with any questions OCIS-Help@unc.edu

Phishing
OCIS continues to receive reports of phishing attempts. To learn how to better spot phishing, see the following guidance https://its.unc.edu/files/2016/10/Anatomy-of-a-Phishing-Email.pdf. 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
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**. *Encryption is one of the few technologies specifically mentioned in HIPAA.* Since Monday, May 1st, OCIS has been rechecking all 688 laptops for HIPAA compliance. **If you have a laptop for use at the SoD, please bring your laptop to OCIS 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. Since Monday, May 1st. OCIS has been distributing these USB keys. For those who are listed for receiving keys, an email notification has been sent.

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 tohttps://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.

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 tohttps://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 90 days since the last reported HIPAA Security Incident. Stay vigilant!**

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
As we continue to experience an increase of finding unencrypted USB Flash Drives in meeting rooms and classrooms, we have to examine every flash drive we find for patient data and report any suspect data found to campus authorities. . We are a HIPAA health care environment. **Please use encrypted USB flash drives**. For information about encrypted flash drives, please contact OCIS. **It has been 90 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: Two-Step Verification
To learn more : 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) 537-3434

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/