OUCH! Newsletter – Password Managers
Creating a unique, strong password is one of the many important steps you can take to protect yourself online. One important aspect to note : re-using the same password is dangerous as your password can easily be used to compromise all of your accounts that use the same password. Please review solutions and recommendations for managing your passwords: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201709_en.pdf

HHS Accelerates development of first Ebola vaccines and drugs
Hundreds of thousands of Americans could be protected or treated for Ebola infections through the first purchase of vaccines and therapeutic drugs by the Biomedical Advanced Research and Development Authority (BARDA), part of the Office of the Assistant Secretary for Preparedness and Response (ASPR) within the U.S. of Health and Human Services. More information as well as other latest news located here: **https://www.hhs.gov/about/news/index.html**

SoD Use of Microsoft 365 OneDrive: Latest news
OCIS will continue providing 1 hour general overview trainings on the advantages and general use of Microsoft OneDrive. As classes are filling up quickly, please continue to you inbox for invitations to sign-up for the classes. **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 email OCIS with any questions OCIS-Help@unc.edu

Laptop Encryption Project Status
OCIS is continuing cycles for checking laptop encryption. If you have not done so already, please bring your laptops down to OCIS for a security re-check (dental school policy and security requirement). **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.** Failure to do so is a violation of HIPAA and University policy.

OCIS Self-service terminal
During the month of August, OCIS has made available a self-service terminal that is available in the front office of the guest area. The goal is to accommodate an efficient process for everyone in the School of Dentistry to submit requests in a visible manner outside of OCIS walk-in hours. For those of you who have begun using the self-service terminal, we hope you are able to take full advantage of the features that are available. If for any reason there are any issues with submitting request, please alert OCIS, OCIS-Help@unc.edu, with any questions or comments that you may have so that we can continue to improve our delivery of self-service.

SoD Security Awareness Training Test Requirement
Thanks to everyone who has worked diligently on completing **the SoD Security Awareness Training.** In order to maintain access to 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/. If you have questions **or run into any issues as you are taking the training,** please contact OCIS Security Officer.

Required Bi-Annual Access Control Auditing
To comply with that requirement of reviewing and auditing access to patient data systems and applications, **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.

HIPAA Security Incident Update
In the month of September, we have received **two** incidents of finding USB Flash Drives found in meeting rooms and classrooms. Since we are a health care environment, we have to examine every incident and report any suspect data found to campus authorities. **Please use encrypted USB flash drives. For information about encrypted flash drives, please work with your department manager.**

OUCH! Archives
For previous issues and topics: https://securingthehuman.sans.org/ouch/archives

Security Awareness Tip of the Day: Email auto-complete : Be Vigilant
To learn more : http://www.sans.org/tip-of-the-day

Remember. It is your personal responsibility to protect patient data (e.g. electronic Protected Health Information) 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.

Safe computing.

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

School of Dentistry Deputy Security Officer
Nefertiti Holland
Email: nefertiti_holland@unc.edu
Phone: (919) 537-3432

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

School of Dentistry Risk Management Office
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/