OUCH! Newsletter – Backup and Recovery
Backups are copies of your information stored somewhere other than on your computer or mobile device. When you lose valuable data, you can recover that data from your backup. If you use a computer or mobile device long enough, sooner or later something will go wrong, resulting in you losing your personal files, documents, or photos. To learn more about taking the first steps to backup and recover your
data: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201708_en.pdf

Secretary Price Travels to Texas to Observe Hurricane Harvey Relief Efforts
U.S. Department of Health and Human Services Secretary tom Price, M.D., traveled with the President today to Texas to see the damage from Hurricane Harvey first-hand; to received briefings on rescue efforts; and to meet with counterparts from the Texas Health and Human Services Commission, Executive commissioner Charles Smith. Across the department, HHS continues to provide support to those affected in Texas and Louisiana by Hurricane Harvey. To learn more on the latest activities HHS has been conducting to help with the current
news: **https://www.hhs.gov/about/news/2017/08/29/secretary-price-travels-texas-to-observe-hurricane-harvey-relief-efforts.html**

Laptop Encryption Project Status
It is that time of year where OCIS Laptop encryption checking is now underway. OCIS has already been servicing dental school members thus far who have brought in their laptops in tandem with receiving encrypted USB keys. **As of Tuesday, September 4th, OCIS will be officially starting the cycles for checking laptop encryption for the new school year.** 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.

SoD Use of Microsoft 365 OneDrive
OCIS has completed its first series of Office 365 trainings for the month of August. As we move into the beginning of September, we are working on coordinating future trainings (date to be determined). OCIS will provide an announcement near-term. Please email OCIS Security with any questions.
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

USB Hardware Encrypted USB Flash Drives Distribution
Thank you to all who have participated in the OCIS security compliance program for USB encrypted flash drive distribution. OCIS has worked diligently during the spring and summer months to ensure success. Your participation in this very important security effort has allowed the School of Dentistry to remain strong in building a defense around the protecting and safeguarding of sensitive data.

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.

SoD Security Awareness Training Test Requirement
Announcements will continue to distribute for those who are overdue on **taking the SoD Security Awareness Training.** If you are receiving emails, **you are overdue.** 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.

HIPAA Security Incident Update
In the month of August, we have received **four** incidents 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.

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

Security Awareness Tip of the Day: Never Respond to Emails asking for Personal Information
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 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/