OUCH! Newsletter – Gaming Online Safely and Securely
Online gaming is a trivial way to have fun; it does come with its own set of risks. As you play and communicate with other gamers around the world, there is substantial risk involved as you are playing and trading information with those of who you may not know. Gaming IS fun, however, there are some steps you should take and keep in mind, for remaining secure. Learn more on remaining viligent: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201707_en.pdf

HHS unveils improved web tool to highlight recent breaches of health information
HHS has publicized a revised web-based tool that empowers individuals to better identify recent breaches of health information as well as to learn how all recent breaches of health information are investigated and successfully resolved. HHS OCR originally released the HBRT in 2009, as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. To learn more on the new features of
HBRT: https://www.hhs.gov/about/news/2017/07/25/hhs-unveils-improved-web-tool-highlight-recent-breaches-health-information.html

SoD Use of Microsoft 365 OneDrive
Beginning in the month of August, OCIS is providing three hands-on information sessions on Office 365. All sessions will be in Brauer 036 – SoD Computer Training Room. As the first two session are full due to high demand, OCIS is now offering two additional hands on sessions on the following dates:
August 8, 2017, 12pm – 1 pm http://doodle.com/poll/u84vzzgu8xwpgthx
August 10, 2017, 12pm – 1 pm http://doodle.com/poll/eawbumm4as7dfrk5
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
As of Monday, May 1st. OCIS has been distributing these USB keys. For those who are listed for receiving keys, an email notification has been sent. **Please continue to monitor email communications for important details regarding deadlines as they apply. If you have a university-owned laptop, please bring your university owned laptop down to OCIS First Dental for security re-check (see below). Your laptop security re-check may be completed at the time of your USB key distribution.**

Laptop Encryption Project Status
As of Monday, May 1st, OCIS has been rechecking all 688 laptops for HIPAA compliance. **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.

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
OCIS is now enforcing the annual SoD Security Awareness Training requirement. Announcement will continue to distribute for those who are overdue on 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 tohttps://www.dentistry.unc.edu/secure/training/securityawareness/. If you have questions, please contact OCIS.

HIPAA Security Incident Update
In the month of July, we have received **one** incident 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 please go here: https://securingthehuman.sans.org/ouch/archives

Security Awareness Tip of the Day: Don't Lose That Device
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) 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/