OUCH! Newsletter – Shopping Online Securely
This month we cover *Shopping Online Securely*. With the holidays coming up, this is the time when millions of people around the world shop online. It's also the time when cyber criminals ramp up their game for online fraud. In this issue we cover how you can easily shop online safely and securely and make the most of all those great online deals. Share this edition with your family, friends, and coworkers.
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201711_en.pdf

Holiday Laptop Purchases?
On the subject of holiday shopping, if you get a new laptop over the holidays and plan to use it here at the SoD, please bring it down to OCIS for a HIPAA security check and if you used your old laptop at the school you must bring it down to OCIS before parting with it. **In all cases, patient data can never be stored on a laptop unless it has been inventoried, encrypted and approved by OCIS.**

Equifax Update
Have you read all about the Equifax hack but are still confused on what exactly happened or what you or your family should do to protect themselves? Find all your answers in this simple guide that gives you the facts and the key steps to take to protect yourself and your family's future. https://securingthehuman.sans.org/blog/2017/09/08/awareness-officers-what-to-communicate-about-the-equifax-hack?

US DHHS Office of Civil Rights in Action – Mobile Devices and Protected Health Information (PHI)
Mobile devices, including cell phones, tablets, and laptops, are increasingly ubiquitous in many work environments – including healthcare organizations like the SoD. The use of mobile devices in the workplace can be convenient and productive, but we should realize the risks associated with increased usage of mobile devices – especially when mobile devices are used to create, receive, maintain or transmit electronic PHI (ePHI). See the full article here
https://www.hhs.gov/sites/default/files/october-2017-ocr-cybersecurity-newsletter.pdf

Office365 Training
OCIS will continue providing one-hour general overview training on the advantages and general use of Office365. As classes are fill up quickly, please monitor your email for invitations to sign-up for the classes. Documentation to Office 365 training and the required SoD attestation is here http://bit.ly/sodo365docs. You may need to login to Office365 using your ONYEN@ad.unc.edu to access the documentation.

Phishing
OCIS still receives 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/

Laptop Encryption Project Status
OCIS has documented the encryption of 204 SoD laptops since January 2017. Additionally, we have emailed 139 encryption "receipts" to customers.

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 Security Awareness Training Test Requirement
To comply with HIPAA and UNC policy, OCIS is 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/. If you have questions, please contact OCIS.

Required Bi-Annual Access Control Auditing
OCIS recently completed the Fall 2017 bi-annual access control audit. As of October 20, 2017, OCIS validated the access level of 96 percent of all EPR accounts.

HIPAA Security Incident Update
The SoD has gone 63 days since the last reported HIPAA security incident. **Good job and stay vigilant!**

2-step authentication is coming
Campus networking and security have notified OCIS that 2-step authentication is coming soon for SoD VPN and Office 365 users. To prepare for this, please go to https://help.unc.edu/help/duo/ to learn how to register for Duo 2-step verification. Stay tuned for more information about 2-step authentication and what will change for you. If you have questions contact OCIS.

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

Security Awareness Tip of the Day: 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
Mauricio Tavares
Email: mtavares@email.unc.edu
Phone: (919) 537-3428

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/