OUCH! Newsletter – Lock Down Your Login

This month we cover *Lock Down Your Login*. Numerous reports, analysis and findings all point to the same conclusion. One of the most effective steps you can take to protect your online lives is enable two-factor authentication whenever possible. **This is very relevant as the University will soon require two-factor authentication for the SoD VPN and soon for using Office 365.** Article is here. https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201712_en.pdf?

Holiday Laptop Purchases?

Happy Holidays! 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.**

US DHHS Office of Civil Rights in Action – Insider Threats and Termination Procedures

Data breaches caused by current and former workforce members are a recurring issue across many industries, including the healthcare industry. Effective identity and access management (IAM) policies and controls are essential to reduce the risks posed by these types of insider threats. IAM can include many processes, but most commonly would include the processes by which appropriate access to data is granted, and eventually terminated, by creating and managing user accounts. Making sure that user accounts are terminated, so that former workforce members don't have access to data, is one important way IAM can help reduce risks posed by insider threats. See the full article here https://www.hhs.gov/sites/default/files/november-cybersecurity-newsletter-11292017.pdf?language=es

2-step authentication is coming

Campus networking and security have notified OCIS that 2-step authentication will be required starting January 2, 2018. To prepare for this, please go to https://help.unc.edu/help/duo/ to learn how to register for Duo 2-step verification. Additionally, campus will begin to require 2-step authentication for Office 365 in early 2018. If you have any questions contact OCIS.

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/

Office365 Training

OCIS has been providing hands-on Office 365 training classes since August 2017. If there is still a need for hands-on Office 365 training, please contact Linda Clark. Documentation to

Office 365 training and the required SoD attestation is here http://bit.ly/sodo365docs. You may need to login to O365 using your ONYEN@ad.unc.edu to access the O365 documentation.

Laptop Encryption Project Status
Since January 2017, OCIS documented the encryption of 277 SoD laptops. Since May 2017 we have validated the encryption of 103 SoD laptops.

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.

HIPAA Security Incident Update
The SoD has gone **95** days since the last reported HIPAA security incident. **Good job and stay vigilant!**

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/