OUCH! Newsletter

This month's security focus is on malware (computer viruses). Specifically, what malware is and the key steps you can take to protect yourself against it.
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_en.pdf

Phishing (Fake Emails)

There has been a marked increase in UNC Phishing attacks with many people writing to me or OCIS team members asking "Is this legitimate?" The fake messages are getting harder to spot and a few folks have been "hooked" by the Phisherman and entered their personal information. ITS has a webpage that shows current Phishing attacks campus-wide. To use it go to http://help.unc.edu/help/caught-a-Phish/

- To forward suspected Phishing or spam messages to campus for evaluation, go here http://help.unc.edu/help/how-to-forward-suspect-Phishing-spam-email-messages-for-evaluation/
- To learn how to spot fake emails like a pro and avoid getting hooked, go here http://help.unc.edu/help/recognizing-and-reporting-fraudulent-emails/
- **If you do get hooked and enter your information into a fake email, immediately change the password of the account your entered and then call OCIS or the ITS help desk for additional instructions.**
- Information from the Department of Homeland Security on Phishing https://www.us-cert.gov/ncas/tips/ST04-014

Encryption

Encryption is one of the few technologies specifically mentioned in HIPAA. It is crucial to encrypt all mobile computing and mobile storage devices that could come into contact with patient data to comply with HIPAA and University policy. OCIS is currently running a project to verify the encryption of all faculty, staff and student laptops and mobile storage. We are currently working with the DDS 2017 class and are preparing to work with the DDS 2018 and 2019 classes. Additionally, OCIS is working with the school's leadership to purchase encrypted USB drives for certain programs, departments and staff. Please contact OCIS if you need more information about encryption.

HIPAA Incident Update

The last reported HIPAA incident was a lost, unencrypted USB flash drive on February 24, 2016. **We have gone 21 days since the last incident. Stay vigilant.**

Secure Email

OCIS in conjunction with the SoD Privacy and Security officers are preparing to announce an approved method to securely send patient information to non-UNC email addresses. Stay tuned for details.

OUCH! Archives

For previous issues and topics please go here:
https://securingthehuman.sans.org/ouch/archives

Security Awareness Tip of the Day
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 or ePHI) 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.

Thanks and 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
Michael Owino
Email: mowino@unc.edu
Phone: (919) 537-3428

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

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/