OUCH! Newsletter

This month's security focus is on the Internet of Things (IoT). Specifically, we discuss what IoT is, how IoT impacts our personal lives, and what we can do to protect IoT devices. Because we bring mobile devices to the School or work from our home networks, this is important for you to know to best protect patient data while working from your home network.

https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201605_en.pdf

Phish Alert!

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/

Encryption Project Status

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 faculty and staff laptops for encryption and attestation. Since January 2016, we have successfully encrypted and verified 420 laptops. If you have an unencrypted laptop, please contact OCIS as soon as possible.

OCIS has recently received 649 encrypted USB flash drives for certain programs, departments and staff. We are currently testing a process to quickly register and distribute these USB flash drives.

Please contact OCIS if you need more information about encryption.

HIPAA Security Incident Update

The last reported HIPAA security incident was a lost, unencrypted USB flash drive on February 24, 2016. **We have gone 78 days since the last HIPAA security incident. Stay vigilant.**

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/