

August 2018

OUCH! NEWSLETTER

Smart Home Devices

This month's OUCH! Newsletter is about smart home devices.



We explain what smart home devices are and how to secure them.

These devices are part of almost everyone's homes and daily lives, yet many of these devices are highly insecure. This problem will only grow worse as smart home devices become the norm for most home appliances or devices. It is important to learn how to leverage these devices, safely and securely.

[Read more about smart home devices here.](#)

Security Awareness Training Test Requirement



In order to comply with HIPAA and UNC-CH policy, OCIS is enforcing the annual School of Dentistry Security Awareness Training requirement.

Laptop Encryption Status



It is not enough for your laptop to be encrypted, we must have documentation and proof of encryption in the event your laptop is lost or stolen.

OCIS is responsible for keeping documentation on the encryption and security of all laptops accessing patient data. If your laptop does not have a SoD tag like this, we may not have a record of it. Please bring your laptop to OCIS immediately for a laptop security check.

REMEMBER: If you have an unencrypted laptop or unencrypted USB flash drive and are using it at the school, contact OCIS as soon as possible! Failure to do so is a violation of HIPAA and University policy. Don't get caught with an unencrypted device.

Phishing

OCIS still receives reports of phishing attempts. [To better spot phishing, click here.](#)

Please forward any phishing messages that you encounter **as an attachment** to

You will be **required** to take and pass both the HIPAA and Security Awareness test in order to access the EPR.

To take the Security Awareness Training and Test [please click here](#). If you have questions, please contact OCIS.



How to Create a Secure Password

Your password is your defense against cyber-criminals. It is important that you choose a long and strong password that cannot be easily cracked. This is especially important for in health care environments like the School of Dentistry.

[Click here for the OCIS recommended guidelines for choosing an effective password.](#)

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 its.unc.edu/phish-alerts/.

US DHHS Office of Civil Rights in Action

[Nothing new this month, but you can read the latest Office of Civil Rights bulletins and an archive of past releases here.](#)



Password Managers

A password manager helps to generate and retrieve complex passwords, potentially storing such passwords in an encrypted database or calculating them on demand.

When selecting a password manager for your personal use, [the UNC-CH Information Security Office recommends you use the matrix given here](#) to evaluate the relative strength of any password manager under consideration.

ATTENTION: Two-Step Authentication is Coming

Recent events at the University are forcing campus to accelerate 2-step authentication for all Office 365 users.

ALL incoming 2018 students will be required to register for 2-

step to access Office 365 -- this includes incoming DDS, DH and graduate students.



Here is the upcoming two-step schedule:

- **October 2018:** Required for students in Office 365 (currently optional)
- **November 2018:** Required for faculty and staff in Office 365 (currently optional)

To set up your 2-step, go to its.unc.edu/2-step/. If you have any questions, contact OCIS.

HIPAA Security Incident Update

The School of Dentistry has gone **26** days since the last reported HIPAA security incident.

Please stay vigilant!

OUCH! Archives

[Click here for prior issues and topics.](#)

Security Awareness 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.



Contact Us

School of Dentistry HIPAA Security Officer

David Rankin

Email: david_rankin@unc.edu

Phone: (919) 537-3485

School of Dentistry HIPAA Privacy Officer (Interim)

Dr. Lisa Stoner

Email: lisa_stoner@unc.edu

Phone: (919) 537-3588

School of Dentistry Deputy Security Officer

Mauricio Tavares

Email: mtavares@unc.edu

Phone: (919) 537-3428

School of Dentistry Risk Management Officer

Martin Folliard

Email: mfolliar@email.unc.edu

Phone: (919) 537-3444

For More Information

The Office of Computing & Information Systems (OCIS)

(919) 537-3500

OCIS-Help@unc.edu

<http://bit.ly/UNC-OCIS>

Connect with us

