UNC | SCHOOL OF DENTISTRY
Computing and Information Systems

March/April 2019

OUCH! NEWSLETTER

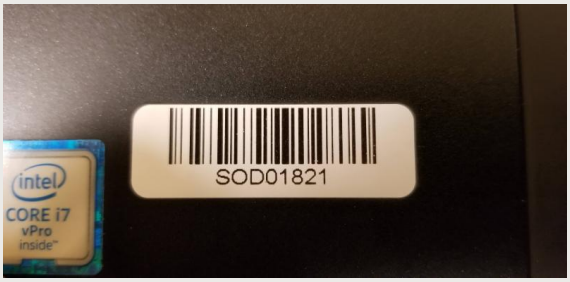
Disposing of Your Mobile Device *and* Making Passwords Simple

People often do not realize how much **personal data** is on their personal devices. Click here to learn what may be on your mobile device and how you should securely wipe it **before** disposing of it.

You are often told your passwords are key to protecting your accounts, but rarely are you given a simple way to securely create and manage all your passwords. Click here to see **three simple steps** to simplify your passwords, lock down your accounts, and protect your future.

Security Awareness Training Test 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 tag like the one above, 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.

Phishing

OCIS still receives reports of phishing attempts. Please forward any phishing messages that you encounter **as an attachment** to phish@unc.edu.

To check and see if you have a suspected phishing email, go to its.unc.edu/phish-

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

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.

alerts/.

For an explanation of how to forward an email as an attachment **please read the following article on help.unc.edu.**

To learn how to better spot phishing, click here.

US DHHS Office of Civil Rights in Action

Touchstone Medical Imaging has agreed to pay $3 million to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS), and to adopt a corrective action plan to settle potential HIPAA violations. Touchstone provides diagnostic medical imaging services in Nebraska, Texas, Colorado, Florida and Arkansas.

In May 2014, Touchstone was notified by the FBI and OCR that one of its FTP servers allowed uncontrolled access to PHI. This uncontrolled access permitted search engines to index the PHI of Touchstone's patients. Touchstone admitted that the PHI of more than 300,000 patients was exposed including, names, birth dates, social security numbers, and addresses.

Two-Step Authentication

2-Step for Office 365 is now being fully enforced at the Adams School of Dentistry. If you are having any problems with your 2-step, please contact OCIS or ITS. To set up your 2-step, go to **https://its.unc.edu/2-step/**.

Change to 1-Year Passwords

UNC-CH has announced a move to 1-year Onyen passwords starting May 13. You will change to a 1-year password the next time your password comes up for renewal on your current cycle.

What to expect

Passwords **cannot**:

- Contain common words or phrases

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 use, **the UNC-CH Information Security Office recommends you use password managers from well known and established companies.**

- linked to UNC (no more references to Carolina, UNC, Tar Heels or your Onyen)
- Be reused for four years
- Include strings from your previous password (Ex: password1# changing to password2#)
- Be in a database of previously hacked passwords

User interface changes

As you type your new password on the website where you change your password, a strength meter will change from red, to orange, to green to tell you how strong your password is. **Click here for more details.**

HIPAA Security Incident Update

The School of Dentistry has gone **83** 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

Adams School of Dentistry HIPAA Security Officer
David Rankin
Email: **david_rankin@unc.edu**
Phone: (919) 537-3485

Adams School of Dentistry HIPAA Privacy and Risk Management Officer
Martin Folliard
Email: **mfolliar@email.unc.edu**
Phone: (919) 537-3444

For More Information

Adams School of Dentistry Policies | UNC-CH Policies | What is Sensitive Information?

The Office of Computing & Information Systems (OCIS)
(919) 537-3500
OCIS-Help@unc.edu
http://bit.ly/UNC-OCIS

Connect with us