

July/August 2019

# OUCH! NEWSLETTER

## New Security Awareness Training Test

All UNC-CH health affairs schools have a [new IT Security Awareness training](#), accessible via SelfService on ConnectCarolina. This training **replaces** all old security awareness training. *Even if you have taken the old training, you will need to complete the new training when contacted by the University's ITS.*



When it is time to take the new training, you will receive an email from Information Technology Services with the subject "Security Awareness Training" and a return address of noreply@unc.edu. Instructions will be included in the email. Questions? Contact the ITS Service Deck at (919) 962-4357.

## Virtual Private Networks (VPNs)

You may need to use public Wi-Fi for Internet access when you are away from the



dentel school. But how secure are these public networks and who is watching or recording what you are doing online? Protect your online activities and privacy with your VPN ([Virtual Private Network](#)). A VPN is a technology that creates a private, encrypted tunnel for your network activity making it much more difficult for anyone to watch or monitor what you are doing online. [Read more about the University's VPN.](#)

## Backups

If you use a computer or

## 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**



mobile device long enough, something will eventually go wrong. You may accidentally

delete the wrong files, have a hardware failure or lose a device. Even worse, malware, such as ransomware, may wipe your files and/or hold them captive. [At times like these, backups are often the only way to rebuild your digital life.](#)

## Security Awareness Training Test Requirement



In order to comply with HIPAA and UNC-CH policy, OCIS is enforcing the annual Adams 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.

Visit ConnectCarolina and select "Self Service" to take the Security Awareness Training and Test. Questions? Contact OCIS.



**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

Please forward any phishing messages that you encounter **as an attachment** to [phish@unc.edu](mailto:phish@unc.edu).

To check and see if you have a suspected phishing email, go to [its.unc.edu/phish-alerts/](https://its.unc.edu/phish-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

Medical Informatics Engineering, Inc. (MIE) has paid **\$100,000** and has agreed take corrective action to settle potential violations of HIPAA Privacy and Security Rules. MIE provides software and electronic medical record services to healthcare providers.

In 2015 MIE discovered that hackers used a compromised user ID and password to access the electronic protected health information (ePHI) of approximately **3.5 million people**. An investigation revealed that MIE did not conduct a comprehensive risk analysis prior to the breach.

## Two-Step Authentication

2-Step for Office 365 is now at the UNC-CH 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/>.

## 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.](#)



## 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.](#)

## Change to 1-Year Passwords

The University announced a move to 1-year Onyen passwords effective 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 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 **43** 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](mailto: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](mailto: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](mailto:OCIS-Help@unc.edu)

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

Connect with us

