UNC | SCHOOL OF DENTISTRY
Computing and Information Systems

May 2018

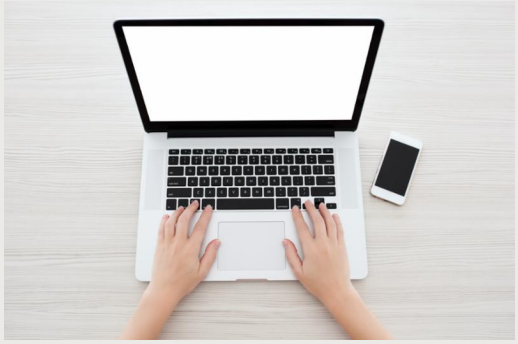
OUCH! NEWSLETTER

What is GDPR?

You may have heard of a new law called GDPR, or the General Data Protection Regulation. This law was developed by the European Union and takes effect May 25, 2018. It applies to any organization that handles the personal information of any resident in the European Union (EU), regardless of where in the world that organization is located. GDPR requires organizations to maintain the privacy and security of any EU resident's personal information. To ensure compliance with GDPR, some key principles need to be understood and implemented. **Read more here.**

Security Awareness Training Test Requirement

Laptop Encryption Project Status



Since **January 2017**, OCIS documented the encryption of **397** laptops. Since **May 2017**, we have validated the encryption of **188** laptops. **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 **phish@unc.edu**. For an explanation of how to forward an email as an attachment **please read the following article on help.unc.edu.**

In order to comply with HIPAA and UNC 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.

Two-Step Authentication Is Coming

Campus networking and security have notified OCIS that two-step authentication is now required (effective January 2, 2018).

Here is the upcoming two-step schedule:

- **May 23, 2018:** Required for ConnectCarolina Administrative Users
- **Fall 2018:** Required for faculty, staff and students in Office 365

To set up your two-step, go to **its.unc.edu/2-step/.**

If you have any questions, 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

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

Risk Analyses vs. Gap Analyses – What's the difference?
HIPAA requires covered entities like the School of Dentistry to safeguard patient data through reasonable and appropriate security measures. A risk analysis is the first step in identifying and implementing safeguards that ensure the confidentiality, integrity, and availability of patient data. A gap analysis is also a useful tool to identify whether certain standards and implementation specifications of the HIPAA Security Rule have been met. **Read more here.**

Plan A. Plan B. Contingency Plan!
The HIPAA Security Rule requires that HIPAA covered entities like the School of Dentistry establish and implement an operational contingency plan. The purpose of any contingency plan is to allow an organization to return to its daily operations as quickly as possible after an unforeseen event. **Read more here.**

Password Managers

A password manager helps to generate and retrieve complex passwords, potentially storing such passwords in an encrypted database

health care environments like the School of Dentistry. **Click here for the OCIS recommended guidelines for choosing an effective password.**

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.

HIPAA Security Incident Update

The School of Dentistry has gone **20** days since the last reported HIPAA security incident.
Good job and 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

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