UNC | ADAMS SCHOOL OF DENTISTRY
Computing and Information Systems

August 2020

OCIS Security Newsletter

Storing Sensitive Information

Over the last 2 months, OCIS has been conducting a survey across the school to determine where users' sensitive information (data such as PHI, FERPA, PII, etc.) is being stored.

Exposure of this data to unauthorized parties could be catastrophic. OCIS highly recommends that sensitive information be stored in authorized storage mediums such as **OneDrive**, **Teams** or the school's **Shared Drive** (i.e. the J drive).

Parties such as Google Drive, Dropbox and in most cases even the local drive of your computer (i.e. Documents, Desktop) are not authorized storage mediums for SI.

For more information on the University's sensitive information standards, click **here** and **here**.

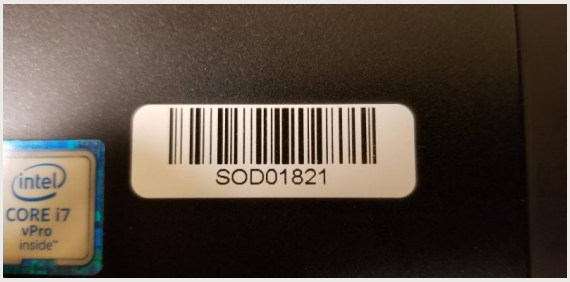
What is Ransomware?

Ransomware is a computer virus that is designed to do exactly what the name sounds like: hold your files and computer hostage until you make a payment to the attacker.

Ransomware has caused some of the worlds most expensive breaches and HIPAA fines. Generally these attacks are start when an infected attachment is opened or a malicious link is clicked.

To avoid ransomare, be sure to enable your anti-virus software, keep your computer and software up-to-date and

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 receives a lot of messages from users asking, "Is this message legitimate?"

If you believe the email you have received is a phishing email, check the UNC Phish Alerts at **its.unc.edu/phish-alerts/**.

most importantly, use cautious judgement with files/emails.

Additionally, utilize OneDrive or teams to store your files rather than storing your data locally!

For more information, click **here**.

Security Awareness Training Test Requirement

When it is time to take your **Security Awareness Training**, you will receive an email from Information Technology Services with the subject "Security Awareness Training" and a return address of noreply@unc.edu. There will be instructions in the email.

To access and complete the training, log in to Connect Carolina. Select "Self Service" and the "Useful Links" tile. There will be a link to the new Security Awareness Training.

Questions? Contact the ITS Service Deck at (919) 962-4357.

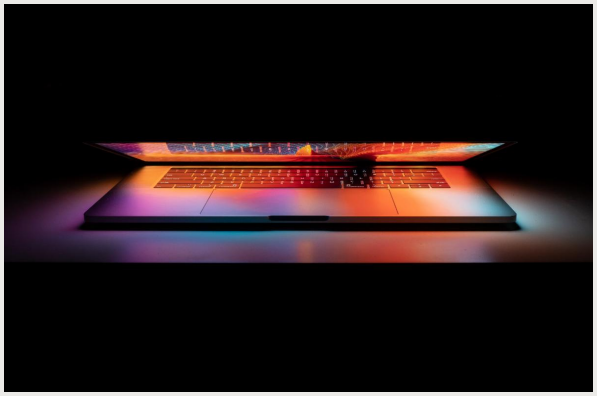
To report a new phishing email, forward any phishing messages that you encounter **as an attachment** to **phish@unc.edu**. To receive feedback about a suspected phishing message, email your question to **security@unc.edu**.

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.

Password Managers

ITS is working on something exciting regarding a University-wide password manager. Stay tuned!



Click here for the Security Awareness Tip of the Day

HIPAA Security Incident Update

The Adams School of Dentistry has gone **39** days since the last reported HIPAA security incident.
Please stay vigilant!

Archives

Click here for prior issues and topics.

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

Adams School of Dentistry
IT Security Analyst
Samuel Garcia
Email: **spgarcia@email.unc.edu**
Phone: (919) 445-2877

For More Information

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