Introduction
The University of North Carolina at Chapel Hill School of Dentistry, during the course of carrying out its teaching, patient care, research and service missions, collects a wide and deep variety of information. Such information includes, but is not limited to, financial, academic, medical/dental, human resources and other forms of personally sensitive data. Federal and State laws have been enacted to protect the confidentiality, integrity and availability of such information relating to Faculty, Staff, Students, Patients and Research Subjects. Further, certain contractual agreements between the School and vendors mandate appropriate levels of safeguarding such information.

Purpose of Policy
To establish a set of reasonable and enforceable measures to ensure Sensitive Information is protected from unauthorized access through the use of data encryption techniques.

Audience
This Policy applies to all Users accessing UNC-Chapel Hill School of Dentistry (SoD) information network(s) using computing devices whether owned or managed through UNC-Chapel Hill or via personally owned devices (see SoD CYOD Policy). This Policy also applies to all UNC School of Dentistry business units that manage or subcontracts their information technology.

Definitions
CYOD(s) – Choose Your Own Device(s) – A personally owned device chosen by the user from a selection of computers picked by OCIS. Students in programs requiring a laptop will choose a computer from models selected by OCIS, and the laptop will be subject to security requirements defined by OCIS.

Computer – An electronic device for storing and processing data according to instructions given to it in a variable program. A computer can be a desktop or portable laptop machine with at least one processing element, typically a central processing unit (CPU), some form of memory and internal hard disk storage.

Computing Device – In the context of computer technology, a device is a unit of hardware, outside or inside the case or housing for the essential computer (processor, memory, and data paths) that is capable of providing input to the essential computer or of receiving output or of both. When the term is used generally (as in computer devices), it can include keyboards, mouse, display monitors, hard disk drives, CD-ROM players, printers, audio speakers and microphones, and other hardware units. Some devices such as a hard disk drive or a CD-ROM drive, while physically inside the computer housing, are considered devices because they are separately installable and replaceable. With notebook and smaller computers, devices tend to be more physically integrated with the “non-device” part of the computer.

Approved on 12/16/2016
UNC-CH School of Dentistry Policy
Encryption

Electronic Storage Media – Any electronic device that can be used to store data. This includes but is not limited to external hard drives and USB flash drives.

Encryption – The process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a “key.”

FERPA - The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.


HIPAA Privacy Rule – The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by “covered entities” (generally, health care clearinghouses, employer sponsored health plans, health insurers and medical service providers that engage in certain transactions).

HITECH Act – The Health Information Technology for Economic and Clinical Health Act was enacted in 2009 to promote and expand the adoption of health information technology. Section D of the act addresses privacy and security concerns associated with the electronic transmission of health information through several provisions that strengthen the civil and criminal enforcement of HIPAA rules.

Information – Knowledge communicated or received concerning a particular fact or circumstance.

Information Owner – A person with statutory or operational authority for specified information (e.g., supporting a specific business function) and responsibility for establishing the controls for its generation, collection, storing, processing, access, dissemination, and disposal.

ISO – Information Security Office

ITS – UNC’s Information Technology Services Department

Laptop Computer – A laptop or notebook computer is a portable personal computer, usually with a clamshell form factor, suitable for mobile use, which functions using a standard operating system (i.e. Windows, the Apple OS or Linux). A laptop combines the components and inputs of a desktop computer, including display, speakers, keyboard and pointing device into a single device.
Mobile Computing Device – A computing device which is a type of computer that can be easily transported and uses batteries to operate, so the device can be used from anywhere, and uses a special mobile operating system. A mobile computing device allows a user to work from any location and access the Internet through a cellular network or a Wi-Fi hotspot. Mobile devices are smaller and more lightweight than traditional computers while still carrying the same functionality.

OCIS – SoD’s Office of Computing and Information Systems.

P2P – Peer-to-Peer file sharing (P2P) allows users to download media files such as music, movies and games using a P2P software client that searches for other connected computers. The “peers” are computer systems connected to each other through the Internet.

Protected Health Information (PHI) – Information covered by the Health Insurance Portability and Accountability Act (HIPAA).

See http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/

Personally Identifiable Information (PII) – Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII. Personally Identifiable Information includes employer tax ID numbers, driver’s license numbers, passport numbers, SSNs, state identification card numbers, credit/debit card numbers, banking account numbers, PIN codes, digital signatures, biometric data, fingerprints, passwords, and any other numbers or information that can be used to access a person’s financial resources.

Public Network – Any network outside the UNC-Chapel Hill network.

Secure Backup – The process of storing information for the purpose of data recovery with security safeguards present to ensure the backup copy of the data remains protected from unauthorized access at all times. Saving data to OCIS servers is considered a secure backup. If a backup is saved to an external drive (portable hard drive, flash drive, etc.), the external drive must have physical protections and encryption to safeguard the information.

Sensitive Information – All data in original or duplicate form which contains:

- HIPAA data (including PHI and PII)
- FERPA data
- Employer tax ID numbers
- Driver’s License numbers
- Passport numbers
- Social Security Numbers

---

1 In this context, ‘computing device’ means a tablet or smartphone.
UNC-CH School of Dentistry Policy
Encryption

- State Identification Card numbers
- Credit/Debit card numbers
- Banking account numbers
- PIN codes
- Digital signatures
- Biometric Data
- Fingerprints
- Passwords
- Any other numbers or information that can be used to access a person’s financial resources

Smartphone – A cellular phone that is able to perform many of the functions of a computer, typically having a relatively large screen and mobile operating system capable of running general-purpose applications.²

SoD – UNC School of Dentistry

Tablet – A tablet computer, or simply tablet, is a mobile computer with a display, circuitry and battery in a single unit. Tablets come equipped with sensors, including cameras, a microphone, an accelerometer and a touchscreen, with finger or stylus gestures substituting for the use of a computer mouse and keyboard.

UNC-ISO – The University Information Security Office. The University’s Information Security Office oversees the security of the University’s electronic information.

University email – UNC’s electronic mail system. UNC’s email is considered by the SoD as sensitive because of the transmission and receipt of HIPAA-related information between SoD faculty, staff, students and external health care providers.

User – A user is a person who uses a computer or network service. A user often has a unique user account identifier (ONYEN). In this context, a User includes, but may not be limited to: all University faculty, students, staff, temporary employees, contractors, outside vendors and visitors to the campus who are authorized to read, enter, copy, query, download or update information.

Policy

Policy Statement

1. University-owned Desktop and Laptop Computers accessing SoD systems shall be registered in the University Active Directory (AD).

² Downloaded from: http://www.oxforddictionaries.com/us/definition/american_english/smartphone

Approved on 12/16/2016
UNC-CH School of Dentistry Policy
Encryption

a. Exceptions may be granted by OCIS on a case by case basis.

2. University-owned laptop computers, and other computers as designated by OCIS, must have their hard drive(s) encrypted using a University-approved encryption software.
   a. Exceptions may be granted by UNC ISO on a case by case basis.

3. Laptops owned by students under the Choose Your Own Device policy must have their hard drive(s) encrypted using a University-approved encryption software.

4. In accordance with the Information Security Standards, part of the Information Security Policy, Sensitive Information must never be stored on a mobile device, including a laptop computer or a smart phone, unless storage on the mobile device has been approved by the Dean.

5. Electronic storage devices, such as USB flash drives and external hard drives, used at the SoD must be encrypted and registered with OCIS.

6. OCIS reserves the right to examine any CYOD laptop prior to a person graduating or leaving the school.
   a. The User/Owner must attest, in writing, there is no Sensitive Information remaining on the computer or any electronic storage device in their possession.

Compliance

Compliance Statement
Due to the possible financial risk and legal consequences associated with the loss of Sensitive Information, failure to comply with this Policy may have serious consequences for employees up to and including terminations of employment. Students who fail to comply with this Policy will be referred to the Honor System, or other disciplinary actions including, but not limited to, probation and dismissal. Contractors and vendors who fail to comply with this Policy may face termination of their business relationships with the University. Violation of this Policy can, in some cases, also carry the risk of civil or criminal penalties.

Roles and Responsibilities
1. Users (as defined above) accessing the SoD computer network shall comply with Federal and State laws and University or School Policies regarding Information Technology security.

2. OCIS shall create, maintain and distribute internal policies and procedures to encrypt existing and new SoD-owned computers and CYOD computers and other devices

Standards to comply with policy
The following ITS Policies are incorporated by reference and made part of this Policy:


Approved on 12/16/2016
1. Information Security Policy
2. Institutional Data Governance Policy
3. Vulnerability Management Policy

The following School of Dentistry Policies are referenced and included in this Policy

1. UNC School of Dentistry Secure Data Policy
2. UNC School of Dentistry Incident Management Plan
3. School of Dentistry Choose Your Own Device Policy

Related Data

Regulations

Contacts

Questions
David B. Rankin, IT Director SoD, Security Liaison SoD 919-537-3485

Violations
David B. Rankin, IT Director SoD, Security Liaison SoD 919-537-3485

Consulting
OCIS Staff, 919-537-3485
UNC Help Desk, 919-962-4357
UNC Information Security Office, 919-445-9393

History

<table>
<thead>
<tr>
<th>Version</th>
<th>Effective Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>01/22/2015</td>
<td>TAD</td>
</tr>
<tr>
<td>2</td>
<td>12/16/2016</td>
<td>GDM</td>
</tr>
</tbody>
</table>

Next Review Date: 12/16/2017

Authorization

Kenneth May, Dean, UNC School of Dentistry

Signature ________________________________________________

Date ___________________________________________________