UNC-CH School of Dentistry  
Secure Data Policy

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 the minimum level of expectations regarding the access and control of sensitive/secure data.

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 subcontract 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(s), 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.

**Custodian** – University officials and their staff who have operational-level responsibility for the capture, maintenance, dissemination and storage of Institutional Data.

**Data** - The representation of discrete facts; any information in electronic or audiovisual format, or any hardware or software that enables the storage and use of such information. The SAA Glossary of Archival and Records Terminology: Facts, ideas, or discrete pieces of information, especially when in the form originally collected and unanalyzed.

**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).

**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.

**Institutional Data** - Institutional Data is a subset of the University’s information resources and administrative records and includes any information in print, electronic or audio-visual format that meets the following criteria:

- Acquired and/or maintained by University employees in performance of official administrative job duties;
UNC-CH School of Dentistry
Secure Data Policy

• Created or updated via use of a University enterprise system or used to update data in an enterprise system;
• Relevant to planning, managing, operating, or auditing a major function at the University;
• Referenced or required for use by more than one organizational unit; and
• Included in official University administrative reports or official University records.

ITS – The University of North Carolina-Chapel Hill Information Technology Services Department.

Mobile Computing Device – A mobile computing device 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 at a Wi-Fi hotspot. Mobile devices are smaller and more lightweight than traditional computers while still carrying the same functionality.

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

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
- 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 an operating system capable of running general-purpose applications.

**SoD** – UNC School of Dentistry

**Stewards** - Senior University officials whose areas have responsibility for managing a segment of the University's Institutional Data resources.

**Tablet** – A tablet computer, or simply tablet, is a mobile computer with 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 computer mouse and keyboard.

**UNC email** – The University’s electronic mail system. University email is considered by the school as sensitive because of the transmission and receipt of HIPAA-related information between faculty, staff, students and external health care providers.
UNC-ISO – The University Information Security Office. The University’s Information Security Office oversees the security of the University’s electronic information.

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
Information, as defined in this policy, in all its forms and throughout its life cycle, will be protected in a manner consistent with its sensitivity and value to the School of Dentistry. Prevention of unauthorized access to sensitive/secure data is the responsibility of all UNC SoD Users. Sensitive/secure data includes, but is not limited to:

1. Personal Health Information (PHI)
2. Personal Identifiable Information (PII)
3. All data in its original and duplicate form as defined by the North Carolina Identity Theft Protection Act of 2004
4. FERPA data
5. UNC Electronic Mail
6. Any other data protected by University policy from unauthorized access includes, but is not limited to:
   a. System access passwords
   b. Some types of research data
   c. Public Safety information
   d. Information concerning select agents
   e. Information Security records
   f. Information File Encryption keys

The University Information Security Policy requires all Users to protect Sensitive Information in all its forms – written, spoken, electronically recorded or printed to be protected from accidental or intentional unauthorized modification, destruction or disclosure.
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 termination 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. Custodian – Conduct periodic audits of Sensitive Information storage locations to ensure no unauthorized access has been attempted or accomplished.
2. System Administrators – Ensure Users are granted the appropriate minimum access to Sensitive Information unless directed by a User Manager.
3. User Manager – Any University administrator, faculty or staff member who supervises Users or who handles School business unit administrative responsibilities. User Managers are responsible for overseeing User access to Sensitive Information including:
   • Review and approval of access authorization requests.
   • Ensure security records are current by initiating security change requests that accurately reflect each User’s role and required access.
   • Ensure approved procedures are followed for employee suspensions, terminations and transfers.
   • Ensure appropriate measures are taken in the event of access privilege revocation.
   • Revoke student, vendor, consultant and others access privileges when such privileges are no longer needed.
   • Provide appropriate training or the opportunity for such training to ensure proper use of computer systems.
   • Promptly report any potential or actual unauthorized access of Sensitive Information to the School of Dentistry HIPAA Security Officer.
   • Follow the directions of the OCIS Director and instructions listed in the SoD Incident Management Plan.
   • Ensure appropriate Policies and instructions are followed for any acquisitions, transfers and surplus of equipment capable of processing or storing electronic information.

---

1 See UNC Information Security Policy
Procedures to comply with policy

1. OCIS has published a set of instructions to help protect unauthorized access to School of Dentistry Information Networks.
2. OCIS has published guidelines to request access to computer systems.
3. All faculty, staff, students and temporary/contract employees are required to complete annual OCIS data security training.

Standards to comply with policy

The following ITS Policies are incorporated by reference and made part of this Policy:

1. UNC-Chapel Hill Campus Standards for Electronic Media Disposal
2. UNC-Chapel Hill Acceptable Use Policy
3. E-Mail Address Policy
4. Incident Management Policy
5. Information Security Policy
6. Institutional Data Governance Policy
7. Password Policy for General Users
8. Transmission of Protected Health Information and Personal Identifying Information Policy
9. Vulnerability Management Policy

Related Data

Statutes

2. Health Information Technology for Economic and Clinical Health Act (HITECH Act)

Contacts

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

Violations
David B. Rankin, IT Director SoD, Security Officer 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 _________________________________________________