UNC
INFORMATION
TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

Transmission of Protected Health Information and Personal Identifying Information Policy

Policy Statement

Protected Health Information (PHI) and Personal Identifying Information (PII) (as defined below) that is transmitted or received by the University of North Carolina at Chapel Hill's (the University's) computer systems, including mobile devices, must be encrypted when transmitted over wireless or Public Networks, including when transmitted via FTP and electronic mail.

Scope

This policy sets forth requirements for the transmission or receipt of Protected Health Information or Personal Identifying Information on the UNC-Chapel Hill network.

Audience

This policy applies to all Users accessing the UNC network or UNC information through computing devices owned or managed through UNC-Chapel Hill or through permission granted by UNC-Chapel Hill. All University faculty, students, staff, temporary employees, contractors, outside vendors and visitors to campus who have access to University-owned or managed information through computing systems or devices are "Users."

Compliance

Due to possible financial risk and legal consequences associated with the loss of Protected Health Information (PHI)and Personal Identifying Information (PII), failure to adhere to this policy may have serious consequences for employees, up to and including termination of employment. Students who fail to adhere to this policy will be referred to the Honor System. Contractors and vendors who fail to adhere to 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.

Definitions

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.

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/

Personal Identifying Information (PII): Personal Identifying Information includes employer tax ID numbers, drivers' 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 info that can be used to access a person's financial resources.

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

Secure Backup (Encryption Recommended): The process of making a backup copy of 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. This may include physical protections as well as encryption to safeguard the backup information.

Reason for Policy

This policy is required to comply with legal requirements regarding the protection of Protected Health Information (PHI) and Personal Identifying Information (PII) from unauthorized access and to protect against data breaches.

Encryption

Examples of when encryption is required include, but are not limited to:

- A University employee, student, contractor, or vendor sending or receiving the University's PHI or PII using his/her home's Internet Service Provider (ISP) connection (e.g.cable company or DSL), unless both (a) using a VPN

connection, and (b) transmitting only to a destination within the campus network..

- Any transmission of PHI or PII sent over any home, public, hotel, or the unsecured campus wireless network, unless both (a) using a VPN connection, and (b) transmitting only to a destination within the campus network. Use of the UNC-Secure campus wireless network does not require VPN as long as one is transmitting to a destination within the campus.
- A University employee, student, contractor, or vendor sending or receiving the University's PHI or PII to a destination address outside the campus network. (Encryption is required in this case, even if a VPN connection is used.)
- Any vendor transmissions of PHI or PII sent over the Internet.
- Use of a PDA to transmit PHI or PII over a Public Network.

Encryption is not *required* for a University employee who uses an on-campus workstation, with a wired connection to the University network, to transmit a document to another University User or to save a document containing PHI or PII to his/her University-managed network folder.

Email encryption will be available to all users of the ITS-provided campus email system in August 2010. Details regarding the use of encryption tools will be made available at that time. The University will not make available an encryption tool for use with handheld devices; however, these tools are commercially available and must meet the encryption standards below.

Encryption standards: Acceptable encryption algorithms include, but are not limited to, Secure Socket Layer (SSL) RC4 128 bit algorithms, SSL ServerGated Cryptography (SGC) 128 bit algorithms, TLS 1.11.128. bit algorithms, or those algorithms that are accepted and certified by the National Institute of Standards and Technology (NIST). Use of a VPN connection satisfies the requirement for encryption only when transmitting PHI or PII to a campus destination. If you have any questions about whether you need to encrypt data or how to encrypt data, please contact the University's Information Security Office at 919-445-9393.

Contacts

Subject	Contact	Telephone	FAX/E-Mail
Policy Questions	The University's Information Security Office	919-445-9393	919-445-9488
Report a Violation			
Request Information Security Consulting			

History

Effective Date:
Revised Date: 6/30/10
Next Review Date: