

UNIVERSITY STANDARD

UNC-Chapel Hill Standard for Transmission of Protected Health Information and Sensitive Information over an External Network or an Unsecure Medium

Purpose and Background

Protected Health Information (PHI) and Sensitive Information (SI) 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 in accordance with the standards detailed in this document when transmitted over external networks or unsecured mediums. This document details the encryption standards required to meet applicable federal, state and University requirements [for University Tier 2 and Tier 3 information](#).

Audience

All users accessing the UNC-Chapel Hill network or UNC-Chapel Hill information through computing devices owned or managed by or with permission granted by the University. All users transmitting business information on behalf of the University.

Standards

PHI and SI must always be encrypted in transit across external networks or unsecured mediums unless a documented exception exists. This means either a secure connection (VPN, HTTPS, etc.) between each endpoint or encryption of the file/information over an unsecure connection.

Questions or special cases may be referred to your unit Information Security Liaison or to the Information Security Office.

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

- Any transmission of PHI or SI sent from an external network such as a home network, or from any external or unsecured wireless network unless using encryption in transmission (VPN, HTTPS, etc.) and transmitting only to a an appropriate, secure destination. Any non-UNC-Secure network is presumed to be unsecure.
- A University employee, student, contractor, or vendor sending or receiving the University's PHI or SI to a destination address outside the campus network.

- Any vendor transmissions of PHI or SI sent over the Internet.
- Use of a smartphone or tablet to transmit PHI or SI.

Use of a VPN or SSL connection to transmit data is not required when the PHI or SI has been demonstrably encrypted as a file or volume using National Institute of Standards and Technology (NIST) approved algorithms and following best practices for key handling and password complexity. Email encryption is available to all users of the ITS-provided campus email system. (For more information on UNC encrypted email use, see <http://help.unc.edu/help/unc-encrypted-email/>.) The University does not make available an encryption tool for use with handheld devices. Many handheld device encryption tools are commercially available; however, to be acceptable for transmitting PHI or SI these tools must meet the encryption standards below.

PHI/SI transmitted using an approved encryption method may only be stored in University-managed network locations or other approved locations such as an approved encrypted mobile device when necessary for University business purposes.

Data encryption is not required when a University employee who uses an on-campus workstation with a wired connection to the University network transmits a document to another University User or saves a document containing PHI or SI to his/her University location that has been approved for PHI/SI storage.

Encryption Standards:

Acceptable encryption methods for the transmission of PHI/SI include, at a minimum, Transport Layer Security (TLS) 1.1 using NIST-approved 128 bit or greater symmetric key algorithms, Internet Protocol Security (IPsec), using algorithms that are accepted and certified by NIST. See <http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf> for more information.

In addition, individual documents may be transmitted if encrypted using any of the NIST-approved algorithms for encryption. Keys should be generated using either UNC's password policy or by using NIST-recommended key generation methods. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133.pdf>.

If you have any questions about compliance with this standard or the encryption of PHI/SI, or have a special case which may require an exception to any part of this standard (which may be issued by the Chief Information Security Officer or their delegate), please contact the University's Information Security Office via 919-962-HELP.

Compliance

Due to possible financial risk and legal consequences associated with the loss of PHI and SI, failure to comply with this standard may put University information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Students who fail to adhere to this standard may be referred to the UNC-Chapel Hill Office of Student Conduct. Contractors, vendors, and others who fail to adhere to this standard may face termination of their business relationships with UNC-Chapel Hill.

Violation of this standard may also carry the risk of civil or criminal penalties.

Roles and Responsibilities

All Users who access, use, or transmit PHI/SI are required to follow this standard, unless an exception is authorized in writing by the Chief Information Security Officer.

Questions of concerns about specific circumstances should be directed to the Office of Information Security via 919-962-HELP.

Definitions

Encryption: The process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge; often referred to as a key or password.

External Network: A network not controlled by the University.

HTTPS: **HTTPS** (also called **HTTP over [TLS](#)**, **HTTP over [SSL](#)**, and **HTTP Secure**) is a [protocol](#) for [secure](#) communication over a [computer network](#) which is widely used on the [Internet](#). HTTPS consists of communication over [Hypertext Transfer Protocol](#) (HTTP) within a connection encrypted by [Transport Layer Security or its predecessor, Secure Sockets Layer](#). The main motivation for HTTPS is [authentication](#) of the visited [website](#) and protection of the [privacy](#) and [integrity](#) of the exchanged data.

Internet Protocol Security (Ipssec): Suite of protocols for securing Internet Protocol (IP) communications at the network layer by authenticating and/or encrypting each IP packet in a data stream. Ipssec also includes protocols for cryptographic key establishment.

Protected Health Information: [Tier 3](#) information covered by the Health Insurance Portability and Accountability Act (HIPAA).

Sensitive Information: Sensitive information is defined as [Tier 2 or 3](#) information that is protected against unwarranted disclosure. See the reference links below for assistance in recognizing and managing sensitive information at the University.

Transport Layer Security: An authentication and security protocol widely implemented in browsers and web servers.

Unsecure Medium: A transmission method, or storage, networking and/or computing device, which does not meet the requirements of a Secure Communication Protocol.

Users: All University affiliates/constituents including, but not limited to, faculty, students, staff, temporary employees, contractors, outside vendors, and visitors to campus who access University-owned or University-managed digital information.

Virtual Private Network (VPN): A virtual network, built on top of existing physical networks, which provides a secure communications tunnel for data and other information transmitted between networks.

Related Documents

[UNC-Chapel Hill Policy on the Transmission of Protected Health Information and Sensitive Information over External Networks or an Unsecure Medium](#)

[UNC Policies and Standards on Passwords for General Users and Systems Administrators](#)

[Health Insurance Portability and Accountability Act \(HIPAA\) Security Rule](#)

[ISO27002 \(guidelines for Information Security within an organization\)](#)

Title: Title: UNC-Chapel Hill Standard for Transmission of Protected Health Information and Sensitive Information over an External Network or an Unsecure Medium

Standard/Procedure Date: October 20, 2015 (20151020)

Last Revision: February 22, 2017 (20170222)

Contacts

Subject	Contact	Telephone	Online/Email
Standards Questions	UNC ITS Information Security Office	919-962-HELP	help.unc.edu
Request Information Security Consulting	UNC ITS Information Security Office	919-962-HELP	help.unc.edu
Questions about “appropriate secure destinations”	Department Information Security Liaison or the UNC ITS Information Security Office	919-962-HELP	https://help.unc.edu/help/information-security-liaisons/
Report a Violation	UNC ITS Information Security Office	919-962-HELP	N/A

Informational Resources: UNC Help & Support: [What is Sensitive Information](#), [UNC Help & Support: Securing Sensitive Information](#) and [UNC Help & Support: Examples of Sensitive Information](#)

Document History

- Effective Date and title of Approver: October 20, 2015, Chief Information Security Officer
- Revision and Review Dates, Change notes, title of Reviewer or Approver: February 22, 2017. Added information regarding the UNC-Chapel Hill Information Classification standard and clarification of examples, Chief Information Security Officer