UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

UNIVERSITY POLICY

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

Policy Statement

Protected Health Information (PHI) and other Sensitive Information (SI) (data classified as Tier 2 or Tier 3 in the UNC-Chapel Hill Information Classification) 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 UNC-Chapel Hill Standard for the Transmission of Protected Health Information and Sensitive Information when transmitted over external networks or an unsecured medium.

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.

Compliance

Due to possible financial risk and legal consequences associated with the loss of PHI and SI, 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 may be referred to the Office of Student Conduct. 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.

Roles and Responsibilities

All users who access, use, or transmit PHI or other data classified as Tier 2 or Tier 3 in the UNC-Chapel Hill Information Classification Standard are required to follow this policy, unless an exception is authorized in writing by the Chief Information Security Officer or delegate.

Questions or concerns about specific circumstances should be directed to the Information Security Office 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.

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.

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.

Related Documents

UNC-Chapel Hill Information Classification Standard

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

Health Insurance Portability and Accountability Act (HIPAA) Security Rule

ISO27002 (guidelines for Information Security within an organization)

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

Contacts

Subject	Contact	Telephone	Online/Email
Policy Questions	UNC ITS Information Security Office	919-962-HELP	help.unc.edu
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: 6/30/2010, Chief Information Officer
- Revision and Review Dates, Change notes, title of Reviewer or Approver:
    a. 10/14/2015 Change in document title, scope change (to Sensitive Information) and removal of Standards to separate document. Chief Information Officer
    b. 2/21/2017 Added reference to Information Classification Standard. Updated links. Chief Information Officer.