



E-Mail Domain Policy

Scope

This Policy sets forth e-mail domain requirements for UNC-Chapel Hill information technology directors or administrators.

Audience

This Policy applies to anyone who manages an Affiliated or HIPAA-Trusted Domain or who seeks to establish an Affiliated or HIPAA-Trusted Domain.

Definitions

Affiliated Domain: An e-mail domain which shares business processes with the University and whose owners agree to provide certain safeguards. Safeguard details are defined in the Memorandum of Understanding for Affiliated Domains.

Alias: An e-mail address that exists solely for the purpose of forwarding to another e-mail address (e.g., the alias john_doe@unc.edu can be used to forward e-mail to jdove@email.unc.edu). E-mail aliases are often used to create convenient replacements for long or difficult-to-remember e-mail addresses. They can also be used to create service-related e-mail addresses such as webmaster@unc.edu.

Auto-Forward: The act of forwarding e-mail through the use of an automated forwarding mechanism. Once configured, these mechanisms forward e-mail from one server to another without any user intervention and/or oversight. Unlike the practice of “Store and Forward” defined below, when a user Auto-Forwards e-mail, a copy of the e-mail message is not maintained by the original e-mail server.

Domain: An internet namespace usually associated with a particular email system. A domain name is the portion of an email address that directly follows the “@” sign (e.g., unc.edu, email.unc.edu, med.unc.edu).

HIPAA: An acronym for the Health Information Portability and Accountability Act, a federal law that governs the use and disclosure of protected health information.

HIPAA Trusted Domain: An on-campus e-mail Domain that provides all of the safeguards of an Affiliated Domain plus added safeguards to satisfy HIPAA



requirements, as defined in the Memorandum of Understanding for HIPAA trusted Domains.

Memorandum of Understanding (MOU) for Affiliated or HIPAA trusted Domains: An agreement between University entities and the Office of Information Security that certain standards will be maintained in order to receive designations that allow wider integration into and use of ITS services.

Onyen: Stands for the "Only Name You'll Ever Need." ITS grants one Onyen per person for access to a variety of University services. It is the login name used by most UNC-Chapel Hill affiliates to log in to online services requiring authentication. See https://onyen.unc.edu/cgi-bin/unc_id/services for more information.

Policy Statement

A department or organization that manages its own e-mail servers may qualify as an Affiliated Domain or a HIPAA trusted Domain. People in these departments may set an Alias (e.g., john_doe@unc.edu) that forwards e-mail messages to either an onyen@email.unc.edu address (e.g., jdoe@email.unc.edu) or to their account in that Affiliated or HIPAA trusted Domain (e.g., jdoe@dev.unc.edu or jdoe@med.unc.edu). Based on the E-mail Address Policy, Auto-Forward is only permitted to another account ending in "unc.edu" and then only as permitted by University policies and procedures as well as federal and state regulations, such as HIPAA.

A. Affiliated Domains

Domains managers may request an Affiliated Domain designation. This designation is required by those entities that manage e-mail services in order to:

- (1) List their Domain addresses in the Campus Directory, and
- (2) Allow employees to Auto-Forward their ITS-managed e-mail Domains (e.g., @unc.edu, @email.unc.edu) to that e-mail Affiliated Domain.

The Affiliated Domain designation requires that responsible parties enter into an MOU with the Office of Information Security. The MOU stipulates that a Domain holder will comply with standard data retention, security, and other administrative best practice.

B. HIPAA Trusted Domains

Schools and departments that are HIPAA covered units may request a



HIPAA Trusted Domain designation. This designation is required for HIPAA covered units that manage their own e-mail services in order to:

- (1) List their Domain addresses in the Campus Directory, and
- (2) Allow employees to Auto-Forward their ITS-managed e-mail Domains (e.g., @unc.edu, @email.unc.edu) to that e-mail Domain.

The HIPAA Trusted Domain designation requires that responsible parties enter into an MOU with the Office of Information Security. The MOU stipulates that a Domain holder will comply with standard data retention, security, and other administrative best practice. This MOU also stipulates additional IT security measures that will be imposed upon HIPAA covered units to ensure that the University is satisfying its responsibility to maintain the privacy of protected health information.

Compliance

Schools or departments that have established an Affiliated Domain or a HIPAA Trusted Domain and subsequently fail to comply with their respective MOU will have their designation rescinded.

Employees who fail to comply with this Policy may face disciplinary action, up to and including termination.

Related Data

ITS Onyen Policy – <http://help.unc.edu/1687>

HIPAA Security Rule –

<http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf>

Email Address Policy –

http://its.unc.edu/ccm/groups/public/@its/@security/documents/content/ccm3_025561.pdf

Information Security Policy -

http://its.unc.edu/ccm/groups/public/@its/documents/content/ccm1_033440.pdf

MOUs for Affiliated and HIPAA domain –

its.unc.edu/ccm/groups/public/@its/documents/content/ccm3_008220.pdf,
its.unc.edu/ccm/groups/public/@it/documents/content/ccm3_008221.pdf



Contacts

Subject	Contact	Telephone	FAX/E-Mail
Affiliated Domain Registration	UNC Information Security Office	919-445-9393	919-445-9488
HIPAA Trusted Domain Registration	UNC Information Security Office	919-445-9393	919-445-9488

History

Effective Date: March 01, 2011
Revised Date: September 16, 2011
Next Review Date: Feb 29, 2012