UNC School of Medicine
Web Publishing Security Policy

Overview

The World Wide Web (WWW) is a key strategic resource for communication, teaching, research and administration and plays a vital role supporting the University of North Carolina School of Medicine's mission. The School of Medicine (SOM) is committed to ensuring the quality, content and accuracy of all information published on SOM Web sites as well as protecting any sensitive information that may be published.

Purpose

The purpose of this policy is to establish guidelines and assign responsibility for anyone authoring, publishing or administering web content data on SOM computers (e.g., central servers, desktops, etc.), to allow safe and effective dissemination of information while complying with University policies, and local, state, and federal laws.

Scope

This policy applies to all faculty, staff and students in all SOM departments, centers, and programs and to their contractors and consultants including those who operate and maintain SOM Web sites.

Policy

1. **Ownership and Responsibilities**
    a. **Head of Unit (e.g., chair/director):** Ultimately responsible for content ownership of that unit's web site and for ensuring that trained staff (e.g., web publishers, web editors and system administrators) are appointed to manage web servers and web space under their control.
    b. **Web Editor:** Responsible for content creation and modification of the web site.
    c. **Web Publisher:** Responsible for content review, ensuring that the content is appropriate for public consumption and verifying that no sensitive information is posted in unsecured space. Other responsibilities include reporting any technical, operational or security problems to management.
    d. **System Administrator:** Responsible for configuring and securing the host system, performing regular backups, implementing security and access controls requested by web site owners, maintaining and evaluating audit logs, and implementing change control procedures for the web server environment.

2. **Content Review and Approval**
    Several areas of content evaluation must be validated and documented:
    a. **Functional testing of file names and links**
    Web Editors and Web Publishers should ensure that data is accessible only to authorized users. Web Publishers are ultimately responsible for validating all functional testing including file names and locations. Editors and Publishers should be aware that information not directly linked from the web site may still be accessible to users via URL hacking (i.e., guessing the URL) and/or URLs appearing within publicly available referrer logs. It is critical to anticipate the kinds of security breaches that might take place and test methods for their prevention.
    b. **Content Review**
    Web Publishers should review all content for potential issues (e.g., policy compliance).

c. **Final Review/Approval**
The Head of Unit/Content Owner should perform a final review and approval prior to content publishing.

While encouraged to post appropriate materials and documents to a properly protected public or private web server, all web editors, web publishers and other content providers must exercise extreme caution to ensure that they do not inappropriately post material that is restricted or prohibited by University policies and local, state and federal laws. Examples of such material include, but are not limited to, HIPAA, FERPA, ADA, NC Identity Theft Protection Act, UNC Health Care Information Security Policy, UNC-Chapel Hill Copyright Policy, and UNC-Chapel Hill Data Network Acceptable Use Policy.

3. Access Controls

Before placing any sensitive or restricted (i.e., not for public consumption) information on a Web server you must:

a. Determine the specific security and protection requirements of all information that you will be posting via the Web site.
b. Determine the users or user groups that have a legitimate need and have been authorized to access the data.
c. Implement one or more technologies to restrict access to the sensitive or restricted information. Examples of technologies available to restrict access to information residing on a Web site are Address-Based Authentication, Basic Authentication, Digest Authentication, Secure Socket Layer (SSL)/Transport Layer Security (TLS).

4. Requirements

a. Anyone authoring, publishing or administering web content information on SOM computers must take the annual SOM HIPAA Online Training Modules: (1) General Privacy and (2) General Information Security.
b. Personal web space is assigned to individual user accounts (e.g., student web space). Personal web pages or any non-university or non-hospital controlled web servers must not contain sensitive information and must comply with the UNC-Chapel Hill Data Network Acceptable Use Policy.
c. All patient information posted on the Web must be de-identified unless absolutely necessary and approved by the head of the unit. Identifiable health information and other sensitive information must be protected using at least Basic Authentication or Digest Authentication in conjunction with SSL. Using only Address-Based Authentication or using Basic or Digest Authentication without implementing SSL in conjunction, is not sufficient for protecting patient or other sensitive information.

5. Best Practice Resources

Until specific technical policy guidelines are formalized for all Internet services, all units that manage a web site should follow best technological practices and are encouraged to consult existing authoritative literature and best practice guidelines such as the W3C - World Wide Web Consortium.

Best practice and guideline materials do not address site-specific issues, which must be taken into account when applied to actual system environments. Experienced technical

personnel should review the settings and test on a non-production system prior to deployment.

Compliance and Enforcement

All web servers and/or web sites are subject to audit by the Information Security Officer. The School of Medicine will enforce its web publishing policy and will take appropriate action should a breach occur. Violations may result in disciplinary or legal action in compliance with School of Medicine and University policies as well as local, state and federal laws.

Definitions and Reference

ADA - The Americans with Disabilities Act, ADA requires all electronic publications, to the extent feasible, must be made accessible to people with disabilities. If it is not feasible, alternative methods must be made available to complete the same tasks. (http://www.usdoj.gov/crt/ada/adahom1.htm)

Address-Based Authentication - Access control is based on an IP address and/or hostname; however, IP spoofing and DNS spoofing limit the effectiveness of these controls. This type of authentication should be used only where minimal security is required, unless it is used in conjunction with stronger authentication methods.

Basic Authentication – uses the Web server content's directory/file access privileges. A requesting user provides a user id and password for access to files in a directory. Security issues with this method are that all password and web content is transmitted in an unencrypted form. This limitation can be overcome by using basic authentication in conjunction with Secure Socket Layer/Transport Layer Security (SSL/TLS).

De-identified – (HIPAA Privacy Standard 164.514 De-identification of protected health information) Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information. Data is de-identified if the following identifiers of the individual or of relatives, employers, or household members of the individual, are removed: Names, all geographic subdivisions smaller than a State (street address, city, county, zip code, etc…), all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older, telephone numbers, fax numbers, electronic mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers, web universal resource locators (URLs), Internet Protocol (IP) address numbers, biometric identifiers including finger and voice prints, full face photographic images and any comparable images, any other unique identifying number, characteristic, or code.

Digest Authentication – Digest authentication is more secure than basic authentication. The user's password is not needed by the server to authenticate, only the hashed value of the user id and password. However, all other data content is sent unencrypted. This limitation can be overcome by using digest authentication in conjunction with SSL/TLS.

FERPA - The Family Educational Rights and Privacy Act, FERPA protects the privacy of "educational records" for current and former students. (http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html)

HIPAA - The Health Insurance Portability and Accountability Act, HIPAA regulates the use and disclosure of individually identifiable health information. The law applies to health care plans, health care providers, and research. (http://www.hipaa.org)

NC Identity Theft Protection Act - No agency of the State or its political subdivisions, or any agent or employee of a government agency, shall intentionally communicate or otherwise make available to the general public a person's personal identifying information. (http://www.ncga.state.nc.us/Sessions/2005/Bills/House/HTML/H1248v6.html)

SSL/TLS – uses a combination of public-key and symmetric key encryption to provide server and client authentication and encryption of communications. A session always begins with an exchange of messages called the handshake. The handshake allows the server to authenticate itself to the client using public-key techniques. This allows the client and the server to cooperate in the creation of symmetric keys used for encryption, decryption and tamper detection during the session that follows. SSL/TLS protects data while in transit; it is not encrypted at either end-point unless additional safeguards are taken at the end-points.

UNC-Chapel Hill Copyright Policy – (http://www.unc.edu/policies/copyrightpolicy2001.pdf)

UNC-Chapel Hill Data Network Acceptable Use Policy – (http://www.unc.edu/policy/aupol.html)

UNC Health Care Information Security Policy - Sensitive information as defined in the policy such as Protected Health Information (PHI), Confidential Information and Internal Information. (http://intranet.unchealthcare.org/site/w3/policies/UNCHCpolicies_pdf/i5.pdf)

W3C – World Wide Web Consortium – http://www.w3.org/

Approved by the HIPAA Planning and Oversight Council – February 26, 2008

Revisions