

HIPAA Privacy

An innovative approach to self-implementation

WorkGroups®

Security Series

Teleconference

Technical Requirements

[Ver 2.0]

Rules and Resources

Wednesday, March 3, 2004
10:00 a.m. – 11:00 a.m., CST



“Security Series (Part IV) – Technical Safeguards”
- Setting the Stage -

Subpart C--Security Standards for the Protection of Electronic Protected Health Information

Sec 164.302. Applicability

Sec 164.304. Definitions

Sec 164.306. Security standards: General rules

- (a) *General requirements*
- (b) Flexibility of approach
- (c) Standards
- (d) Implementation specifications
- (e) Maintenance

Sec 164.308. Administrative safeguards

- (a)
 - * * *
 - (4) (i) Standard: Information access management
 - (ii) Implementation specifications:
 - (A) Isolating health care clearinghouse functions (Required)
 - (B) Access authorization (Addressable)
 - (C) Access establishment and modification (Addressable)
 - (5) (i) Standard: Security awareness and training
 - (ii) Implementation specifications
 - * * *
 - (B) Protection from malicious software (Addressable)
 - (C) Log-in monitoring (Addressable)
 - (D) Password management (Addressable)
 - (6) (i) Standard: Security incident procedures
 - (ii) Implementation specification: Response and Reporting (Required)
 - (7) (i) Standard: Contingency plan
 - (ii) Implementation specifications:
 - (A) Data backup plan (Required)
 - * * *

Sec 164.310. Physical safeguards

- * * *
- (c) Standard: Workstation security.
- * * *

Sec 164.312. Technical safeguards

- (a) (1) Standard: Access control.
- (2) Implementation specifications:
 - (i) Unique user identification (Required).
 - (ii) Emergency access procedure (Required).
 - (iii) Automatic logoff (Addressable).
 - (iv) Encryption and decryption (Addressable).
- (b) Standard: Audit controls.
- (c) (1) Standard: Integrity.

- (2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable).
- (d) Standard: Person or entity authentication.
- (e) (1) Standard: Transmission security.
 - (2) Implementation specifications:
 - (i) Integrity controls (Addressable).
 - (ii) Encryption (Addressable).

Sec 164.314. Organizational requirements

Sec 164.316. Policies and procedures and documentation requirements

Sec 164.318. Compliance dates for the initial implementation of the security standards

HIPAA Security Policy 16 - Technical Safeguards, Person or Entity Authentication Policy

**WASHINGTON UNIVERSITY
HIPAA Security Policy #16**

**Technical Safeguards
Person or Entity Authentication Policy**

Statement of Policy

Washington University and its member organizations (collectively, "Washington University" or "WU") are committed to conducting business in compliance with all applicable laws, regulations and WU policies. WU has adopted this policy to set forth the authentication requirements for access to WU EPHI.

Scope of Policy

The scope of this Policy covers the procedures to be implemented by each WU Business Unit that is a HIPAA health care component to verify that a person or entity seeking access to EPHI is the person or entity claimed.

Policy

- 1) Workforce members seeking access to any network, system, or application that contains EPHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity. (See HIPAA Security Policy #13 - Access Control and HIPAA Security Policy #5 -Security Awareness and Training).
- 2) Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and Password, smart card, or other authentication information.
- 3) Workforce members are not permitted to allow other persons or entities to use their unique User ID and password, smart card, or other authentication information.
- 4) A reasonable effort must be made to verify the identity of the receiving person or entity prior to transmitting EPHI. (Refer to accompanying procedure template for examples)
- 5) Each Business Unit must establish and document procedures documenting for each of the aforementioned requirements and submit such procedures for approval to the HIPAA Security Office.

Creation Date: January 15, 2004

Effective Date: April 14, 2004

Last Revision Date: January 21, 2004

HIPAA Security Policy 14 - Technical Safeguards, Audit Controls Policy**WASHINGTON UNIVERSITY
HIPAA Security Policy #14****Technical Safeguards
Audit Controls Policy****Statement of Policy**

Washington University and its member organizations (collectively, "Washington University" or "WU") are committed to conducting business in compliance with all applicable laws, regulations and WU policies. WU has adopted this policy to set forth the internal audit procedures for security of EPHI that each Business Unit must implement..

Scope of Policy

The scope of this Policy covers the hardware, software and/or procedural mechanisms that will be implemented by WU Business Units to record and examine activity in information systems that contain or use EPHI.

Policy**1) Audit Control Mechanisms**

- a) Each Business Unit with systems containing medium and high risk EPHI must utilize a mechanism to log and store system activity.
- (b) Each system's audit log **must** include, but is not limited to, User ID, Login Date/Time, and Activity Time. Audit logs **may** include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity.
- (c) System audit logs must be reviewed on a regular basis. (See HIPAA Security Policy #2 - Security Management).
- d) Implementation of an audit control mechanism for systems containing low risk EPHI is not required.

2) Audit Control and Review Plan

An Audit Control and Review Plan must be developed by each Business Unit and approved by the HIPAA Security Office. If the Business Unit's EPHI inventory changes, its Audit Control and Review Plan must be reevaluated and resubmitted to the HIPAA Security Office. The plan must include:

- ? Systems and applications to be logged
- ? Information to be logged for each system
- ? Log-in reports for each system
- ? Procedures to review all audit logs and activity reports

Creation Date: January 15, 2004

Effective Date: April 14, 2004

Last Revision Date: January 21, 2004

10.3.1.7 - HIPAA Security Automatic Logoff Policy

10.3.1.7

**Title:** HIPAA Security Automatic Logoff Policy**Policy Number:** 10.3.1.7 (1)

Policy Provisions: To ensure that access to all servers and workstations that access, transmit, receive, or store EPHI is appropriately controlled, the following procedures must be followed:

- Servers, workstations, or other computer systems containing EPHI repositories that have been classified as high risk (See [HIPAA Security Risk Analysis and Mitigation Policy](#) – 10.1.1.1) must employ inactivity timers or automatic logoff mechanisms. The aforementioned systems must terminate a user session after a maximum of, but not limited to, 15 minutes of inactivity.
- Servers, workstations, or other computer systems located in open, common, or otherwise insecure areas, that access, transmit, receive, or store EPHI must employ inactivity timers or automatic logoff mechanisms. (I.E. Password protected screen saver that blacks out screen activity.) The aforementioned systems must terminate a user session after a maximum of, but not limited to, 15 minutes of inactivity.
- Applications and databases using EPHI, such Electronic Medical Records (EMR), must employ inactivity timers or automatic session logoff mechanisms. The aforementioned application sessions must automatically terminate after a maximum of, but not limited to, 30 minutes of inactivity.
- Servers, workstations, or other computer systems that access, transmit, receive, or store EPHI, and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.
- If a system requires the use of an inactivity timer or automatic logoff mechanism as detailed in the aforementioned procedures, but does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:
 - o The system must be upgraded or moved to support the minimum HIPAA Security Automatic Logoff procedures.
 - o The system must be moved into a secure environment.
 - o All EPHI must be removed and relocated to a system that supports the minimum HIPAA Security Automatic Logoff procedures.
- When leaving a server, workstation, or other computer system unattended, workforce members must lock or activate the systems Automatic Logoff Mechanism (e.g. CNTL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing EPHI.

This policy includes, but is not limited to, the aforementioned procedures. This policy and its procedures must be reviewed and evaluated on a periodic basis to ensure that they maintain their technical viability and effectiveness. (See [HIPAA Security Evaluation of Compliance Procedures Policy](#), 10.1.8)

Non-compliance with this policy may result in immediate disciplinary action, up to and including termination of employment and criminal prosecution. (See [HIPAA Security Sanction Policy](#), 10.1.1.2)

Creation Date: September 2, 2003**Date of Last Edit:** October 31, 2003**Recommended By:** Washington University HIPAA Security Committee (WUHSC)**Issue Date:****Effective Date:** April 20, 2005**Authorized By:**

HIPAA Security Policy 17 - Technical Safeguards, Transmission Security Policy**WASHINGTON UNIVERSITY
HIPAA Security Policy #17****Technical Safeguards
Transmission Security Policy****Statement of Policy**

Washington University and its member organizations (collectively, "Washington University" or "WU") are committed to conducting business in compliance with all applicable laws, regulations and WU policies. WU has adopted this policy to outline the requirements for transmission of WU EPHI to ensure the security and integrity of such EPHI.

Scope of Policy

The scope of this Policy covers the technical security measures that each Business Unit that is a HIPAA covered entity component part will implement to guard against unauthorized access to or modification of EPHI that is being transmitted over an electronic communications network or via any form of removable media.

Policy**1) EPHI Transmissions to Non-WU and Carenet Entities**

- a) To appropriately guard against unauthorized access to or modification of EPHI that is being transmitted from WU (Washington University Clinical Operations Network -WUCON- or .wustl.edu) or the BJC Carenet domains to a network outside of such networks, the procedures outlined in this Paragraph 1) must be implemented.
- b) All transmissions of EPHI from the Washington University (WUCON or .wustl.edu) or BJC Carenet domains to a network outside of the aforementioned networks must utilize an encryption mechanism between the sending and receiving entities or the file, document, or folder containing said EPHI must be encrypted before transmission.
- c) Prior to transmitting EPHI from the Washington University (WUCON or .wustl.edu) or BJC Carenet domains to a network outside of the aforementioned networks the receiving person or entity must be authenticated. (see HIPAA Security Policy #16 - Person or Identity Authentication).
- d) All transmissions of EPHI from the Washington University (WUCON or .wustl.edu) or BJC Carenet domains to a network outside of the aforementioned networks should include only the minimum amount of PHI. (See HIPAA Privacy Policy # 11 - Minimum Necessary Request, Use or Disclosure of Protected Health Information).
- e) For transmission of EPHI from the Washington University (WUCON or .wustl.edu) or BJC Carenet domains to a network outside of the aforementioned networks utilizing an email or messaging system, see Paragraph 5 below.

2) EPHI Transmissions between WUCON and Other WU Entities

- a) When transmitting EPHI over an electronic network between WUCON and a .wustl.edu entity, the EPHI

must be password protected or encrypted before transmission as described below.

- b) All transmissions of EPHI from the Washington University (.wustl.edu) domain into the WUCON network must utilize an encryption mechanism.
- c) All transmissions of EPHI from WUCON into the Washington University (.wustl.edu) domain must utilize a mechanism to encrypt or password-protect the EPHI.
- d) All transmissions from WUCON into the Washington University (.wustl.edu) domain that do not contain EPHI require no additional security mechanisms.

3) EPHI Transmissions between WU and Carenet

- a) The WUCON and BJC Carenet networks provide a tiered security architecture protecting EPHI from internal and external vulnerabilities. Therefore, all transmissions of EPHI between the WUCON and Carenet networks are permitted with no additional security mechanisms.
- b) Direct transmissions from the .wustl.edu domain to Carenet are not permitted. All transmissions from .wustl.edu destined for Carenet must authenticate to and go through the WUCON network.

4) EPHI Transmissions Using Electronic Removable Media

- a) When transmitting EPHI via removable media, including but not limited to, floppy disks, CD ROM, memory cards, magnetic tape and removable hard drives, the sending party must:

- ? Use an encryption mechanism to protect against unauthorized access or modification
- ? Authenticate the person or entity requesting said EPHI in accordance with HIPAA Security Policy #16- Person or Entity Authentication
- ? Send the minimum amount of said EPHI required by the receiving person or entity. (See HIPAA Privacy Policy # 11 - Minimum Necessary Request, Use or Disclosure of Protected Health Information)

- b) If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, no additional security mechanisms are required.

5) EPHI Transmissions Using Email or Messaging Systems

- a) The transmission of EPHI from Washington University to a patient via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

- ? The patient has been made fully aware of the risks associated with transmitting EPHI via email or messaging systems.
- ? The patient has formally authorized Washington University to utilize an email or messaging system to transmit EPHI to them.
- ? The patient's identity has been authenticated.
- ? The email or message contains no excessive history or attachments.

- b) The transmission of EPHI from Washington University to an outside entity via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

- ? The receiving entity has been authenticated.

- ? The receiving entity is aware of the transmission and is ready to receive said transmission.
- ? The sender and receiver are able to implement a compatible encryption mechanism.
- ? All attachments containing EPHI are encrypted.

c) The transmission of EPHI within Washington University (See HIPAA Security Policy #13 - Access Control, paragraph #3) via an email or messaging system is permitted without additional security measures or safeguards so long as only a minimal amount of EPHI is being transmitted and the EPHI is not high risk, sensitive or critical. EPHI that is high risk, sensitive or critical should not be sent through clear text email; such EPHI should be sent via encrypted attachment or other secure measure as described in paragraph 5b) above. If an email or message includes an attachment that contains EPHI, the attachment must be encrypted or password protected before transmission.

d) Email accounts that are used to send or receive EPHI must not be forwarded to non-Washington University accounts.

6) EPHI Transmissions Using Wireless LANs and Devices

a) The transmission of EPHI over a wireless network within the Washington University (WUCON and .wustl.edu) and BJC (.carenet.org) domains is permitted if the following conditions are met:

? The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized.

? The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network.

b) If transmitting EPHI over a wireless network that is not utilizing an authentication and encryption mechanism, the EPHI must be encrypted before transmission.

c) The authentication and encryption security mechanisms implemented on wireless networks within the Washington University and BJC domains are only effective within those networks. When transmitting outside of those wireless networks, additional and appropriate security measures must be implemented in accordance with this Policy.

7) Additional Requirements

a) All encryptions mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.

b) When transmitting EPHI electronically, regardless of the transmission system being used, Workforce members must take reasonable precautions to ensure that the receiving party is who they claim to be and has a legitimate need for the EPHI requested.

c) If the EPHI being transmitted is not to be used for treatment, payment or health care operations, only the minimum required amount of PHI should be transmitted. (See HIPAA Privacy Policy #11- Minimum Necessary Request, Use or Disclosure of Protected Health Information.)

Creation Date: January 15, 2004

Effective Date: April 14, 2004

Last Revision Date: January 21, 2004

10.3.1.8 - HIPAA Security EPHI Encryption Policy

10.3.1.8

**Title:** HIPAA Security EPHI Encryption Policy**Policy Number:** 10.3.1.8 (1)

Policy Provisions: To ensure that access to all servers, workstations, and other systems that access, transmit, receive, or store EPHI is appropriately secure, Washington University has instituted the following access control policies:

- [HIPAA Security Unique User Identification Policy](#) – 10.3.1.1
- [HIPAA Security Password Structure Policy](#) – 10.3.1.2
- [HIPAA Security Firewall Use Policy](#) – 10.3.1.4
- [HIPAA Security Wireless Access Policy](#) – 10.3.1.5
- [HIPAA Security Remote Access Policy](#) – 10.3.1.6
- [HIPAA Security Automatic Logoff Policy](#) – 10.3.1.7

The implementation of the aforementioned policies will ensure that access to EPHI and its associated applications, systems, and networks are appropriately secured and controlled. Encryption of EPHI as an access control mechanism is not required unless the custodian of said EPHI deems the data to be highly critical or sensitive. Encryption of EPHI is required in some instances as a transmission control and integrity mechanism. (See [HIPAA Transmission Security Policy](#) – 10.3.5 and [HIPAA Security EPHI Integrity Controls Policy](#) – 10.3.5.1)

This policy includes, but is not limited to, the aforementioned procedures. This policy and its procedures must be reviewed and evaluated on a periodic basis to ensure that they maintain their technical viability and effectiveness. (See [HIPAA Security Evaluation of Compliance Procedures Policy](#), 10.1.8)

Non-compliance with this policy may result in immediate disciplinary action, up to and including termination of employment and criminal prosecution. (See [HIPAA Security Sanction Policy](#), 10.1.1.2)

Creation Date: September 4, 2003**Date of Last Edit:** October 30, 2003**Recommended By:** Washington University HIPAA Security Committee (WUHSC)**Issue Date:****Effective Date:** April 20, 2005**Authorized By:**

10.3.1.6 - HIPAA Security Remote Access Policy



Title: HIPAA Security Remote Access Policy

Policy Number: 10.3.1.6 (1)

Policy Provisions: To ensure that all networks that contain EPHI based systems and applications are appropriately secured, the following remote access policies and procedures must be followed:

- Dialup connections directly into secure networks are considered to be secure connections and do not require a VPN connection. This implementation of secure remote access extends the secure network to the remote user using a secure PSTN (Public Switched Telephone Network) connection.
- Authentication and encryption mechanisms are required for all remote access sessions to networks containing EPHI via an ISP (Internet service provider) or dialup connection. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and secured Citrix client access.
- The following security measures must be implemented for any remote access connection into a secure network containing EPHI:
 - o Mechanisms to bypass authorized remote access mechanisms are strictly prohibited. For example, remote control software and applications such as PC Anywhere or GoToMyPC.com are not permitted.
 - o Remote access systems must employ a mechanism to “clear out” cache and other session information upon termination of session.
 - o Remote access workstations must employ a virus detection and protection mechanism. (See [HIPAA Security Policy # 11 – Server, Desktop, and Wireless Computer System Security](#))
 - o Users of remote workstations must comply with [HIPAA Security Policy # 10 - Workstation Use](#))
- VPN split-tunneling is not permitted for connections originating from outside the University network (WUCON or .wustl.edu) or from an insecure network within the Washington University domain.
- All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.
- The business unit of any workforce member requesting remote access to a secure network containing EPHI-based systems and applications must ensure that the remote workstation device being used by said workforce member meets the security measures detailed in HIPAA Security Policy # 11 – Server, Desktop, and Wireless Computer System Security. The owner (managing entity; MSCNS, Neurology, etc.) of the secure network must ensure that the previous requirement has been satisfied before access is granted.
- Each business unit must establish a formal, documented procedure to ensure that remote workstations and mobile devices used by their workforce members to remotely access secure networks containing EPHI-based systems and applications continue to meet the security measures detailed in HIPAA Security Policy # 11 – Server, Desktop, and Wireless Computer System Security.

This policy includes, but is not limited to, the aforementioned procedures. This policy and its procedures must be reviewed and evaluated on a periodic basis to ensure that they maintain their technical viability and effectiveness. (See [HIPAA Security Evaluation of Compliance Procedures Policy, 10.1.8](#))

Non-compliance with this policy may result in immediate disciplinary action, up to and including termination of employment and criminal prosecution. (See [HIPAA Security Sanction Policy, 10.1.1.2](#))

Creation Date: November 17, 2003

Date of Last Edit: February 11, 2004

Recommended By: Washington University HIPAA Security Committee (WUHSC)

Issue Date: **Effective Date:** April 20, 2005 **Authorized By:**

10.3.1.5 - HIPAA Security Wireless Access Policy

10.3.1.5



Title: HIPAA Security Wireless Access Policy

Policy Number: 10.3.1.5 (1)

Policy Provisions: To ensure that all networks that contain EPHI based systems and applications are appropriately secured, the following wireless access policies and procedures must be followed:

- Wireless access to networks containing EPHI-based systems and applications is permitted so long as the following security measures have been implemented:
 - o Encryption must be enabled. (See [HIPAA Security Use of Wireless LANs and Devices to Transmit EPHI Policy – 10.3.5.3](#))
 - o MAC-based or User ID/Password authentication must be enabled. MAC-based (Media Access Control) authentication is based on a permitted list of hardware addresses that can access the wireless network. MAC addresses are hard coded on each network interface card and typically cannot be changed.
 - o All console and other management interfaces have been appropriately secured or disabled.
- Unmanaged, ad-hoc, or rogue wireless access points are not permitted on any secure network containing EPHI-based systems and applications.
- We recognize that all wireless LANs do not utilize standard 2.4GHz, 5.0GHz or microwave radio frequencies. Wireless LANs and devices may utilize infrared frequencies and may not support the typical wireless LAN encryption and security mechanisms. For instance, the use of infrared ports on PDAs, laptops, and printers to transmit EPHI may not allow encryption of that data stream. We consider this to be a low risk concern because this implementation of infrared is very short distance and low power.
- All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.

This policy includes, but is not limited to, the aforementioned procedures. This policy and its procedures must be reviewed and evaluated on a periodic basis to ensure that they maintain their technical viability and effectiveness. (See [HIPAA Security Evaluation of Compliance Procedures Policy, 10.1.8](#))

Non-compliance with this policy may result in immediate disciplinary action, up to and including termination of employment and criminal prosecution. (See [HIPAA Security Sanction Policy, 10.1.1.2](#))

Creation Date: November 5, 2003

Date of Last Edit: November 24, 2003

Recommended By: Washington University HIPAA Security Committee (WUHSC)

Issue Date:

Effective Date: April 20, 2005

Authorized By:

Security Resource Websites

National Institute of Standards and Technology

Computer Security Resource Center

<http://csrc.nist.gov/>

Automated Security Self-Evaluation Tool

http://csrc.nist.gov/asset/asset_download.html

Information Technology Security: Practices & Checklists / Implementation Guides

<http://csrc.nist.gov/pcig/cig.html>

WEDi – SNIP

Security and Privacy White Papers and PowerPoint Presentations

http://www.wedi.org/snip/public/articles/dis_publicDisplay.cfm?docType=6&wptype=2

Security Policies and Procedures White Paper, Version 2.0 - 11/07/03

<http://www.wedi.org/cmsUploads/pdfUpload/WhitePaper/pub/SPandP2.pdf>

American Health Information Management Association Practice Briefs Public Archive

- 02/2004 - Electronic Record, Electronic Security
Hagland, Mark. *Journal of AHIMA* 75, no.2, p. 18-22.
http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_022425.html
- 01/2004 - HIPAA and the EHR: Making Technical Safeguard Changes
Fodor, Joseph. *Journal of AHIMA* 75, no.1 p. 54-55.
- 02/2004 - The 10 Security Domains
Dougherty, Michelle. "" (AHIMA Practice Brief) *Journal of AHIMA* 75, no.2 p. 56A-D
- 11/2003 - AHIMA Practice Brief: Security Audits
Hjort, Beth. (Updated November 2003)
- 11/2003 - AHIMA Practice Brief: HIPAA Privacy and Security Training
Hjort, Beth. (Updated November 2003)
- 11/2003 - AHIMA Practice Brief: Information Security--an Overview
Quinsey, Carol Ann, and Mary D. Brandt. (Updated November 2003)
- 10/20/03 - Implementing Electronic Signatures
AHIMA Task Force
http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_021585.html

- 10/2/03 - Security Risk Analysis and Management: an Overview
Amatayakul, Margret
http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_021089.html
- 6/27/03 - Disaster Planning for Health Information (Updated)
Burrington-Brown, Jill, Hughes, Gwen
http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_019242.html
- 6/15/03 - Provider-Patient E-Mail Security
Burrington-Brown, Jill, Hughes, Gwen
http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_019873.html
- 6/15/03 - Portable Computer Security (Updated)
Quinsey, Carol, Hughes, Gwen
http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_019872.html
- 6/15/03 - Transfer of Patient Health Information Across the Continuum (Updated)
Hughes, Gwen
http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_019871.html

See also:

Commonwealth of Massachusetts Information Technology Division

<http://www.state.ma.us/itd/spg/publications/standards/index.htm>

**HCA – Hospital Corporation of America
Ethics and Compliance**

<http://ec.hcahealthcare.com/CustomPage.asp?PageName=Policies>

American National Standards Institute

<http://www.ansi.org>

International Organization for Standardization

<http://www.iso.org>

The National Security Agency

<http://www.nsa.gov/snac/index.html>

NH/VT HIPAA security working group

www.nhvship.org

North Carolina Healthcare Information and Communications Alliance, Inc.

<http://www.nchica.org/>

Other Websites with Information Security Policies

<http://www.security.kirion.net/securitypolicy/>
<http://www.network-and-it-security-policies.com/>
http://www.brown.edu/Research/Unix_Admin/cuisp/
<http://iatservices.missouri.edu/security/>
<http://www.utoronto.ca/security/policies.html>
http://irm.cit.nih.gov/security/sec_policy.html
<http://w3.arizona.edu/~security/pandp.htm>
<http://secinf.net/ipolicye.html>
<http://ist-socrates.berkeley.edu:2002/pols.html>

http://www.ruskwig.com/security_policies.htm

<http://razor.bindview.com/publish/presentations/InfoCarePart2.html>

based on the SANS Institute Security Policy Project
<http://www.sans.org/resources/policies/#resources>

Gregory D. Frost
Adams and Reese, LLP

Prior to joining Adams and Reese, Gregory D. Frost was a partner in a Baton Rouge based law firm, where he concentrated his legal practice on health care law, including the representation of physicians; not-for-profit, for-profit and governmental hospitals; other types of health care providers; and health care trade associations. Mr. Frost is experienced in HIPAA and health information issues, licensure and other regulatory matters, Medicare, Medicaid and workers' compensation reimbursement issues, defense of civil and criminal fraud prosecutions, transactional matters and litigation involving health care providers.

Mr. Frost was vice president of Legal and Governmental Affairs of the Louisiana Hospital Association for over eight years. He has lectured at Louisiana State University, Tulane University and the University of Louisiana at Lafayette and regularly speaks before trade and professional organizations and legal audiences. Mr. Frost served on the adjunct faculty of the College of St. Francis and is the organizer of the HIPAA Privacy WorkGroups. In addition to numerous articles on health law issues, he is the editor of *Louisiana Medical Records Law*, which is currently in use as a textbook at two Louisiana colleges. He has also edited *Managed Care, Collections and Related Issues*, and the *Workers' Comp Medicals Handbooks*. Mr. Frost is currently president of the Louisiana Society of Hospital Attorneys, and is a member of the American Health Lawyers Association, the Association of Louisiana Lobbyists and the Louisiana State and Baton Rouge Bar Associations.

451 Laurel Street
19th Floor North
Baton Rouge, Louisiana 70801
225-336-5200

frostgd@arlaw.com



Network Solution Providers specializes in developing customized network solutions for a select group of businesses in central Louisiana. We act as a single point of contact for small to medium size businesses that do not need a full time IT staff. We provide services such as designing networks to meet security needs and developing custom applications to streamline business processes in addition to providing a full range of IT technical support.



www.NSP.cc

Travis Planchard, CEO

tplanchard@nsp.cc

Office - 225.709.2591

Fax - 225.709.2592