

# HIPAA Privacy

*An innovative approach to self-implementation*

# WorkGroups®

## Security Series

### Teleconference

# Physical & Organizational Requirements

*[Ver 2.0]*

## Rules and Resources

Wednesday, February 18, 2004  
10:00 a.m. – 11:00 a.m., CST



**“Security Series (Part III) – Physical & Organizational Requirements”**  
**- 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**

\* \* \*

- (b) (1) Standard: Business associate contracts and other arrangements

**Sec 164.310. Physical safeguards**

- (a) (1) Standard: Facility access controls.
- (2) Implementation specifications:
  - (i) Contingency operations (Addressable).
  - (ii) Facility security plan (Addressable).
  - (iii) Access control and validation procedures (Addressable).
  - (iv) Maintenance records (Addressable).
- (b) Standard: Workstation use.
- (c) Standard: Workstation security.
- (d) (1) Standard: Device and media controls.
- (2) Implementations:
  - (i) Disposal (Required).
  - (ii) Media re-use (Required).
  - (iii) Accountability (Addressable).
  - (iv) Data backup and storage (Addressable).

**Sec 164.312. Technical safeguards**

**Sec 164.314. Organizational requirements**

- (a) (1) Standard: Business associate contracts or other arrangements
- (2) Implementation specifications (Required)
  - (i) Business associate contracts
  - (ii) Other arrangements
- (b) (1) Standard: Requirements for group health plans
- (2) Implementation specifications (Required)

**Sec 164.316. Policies and procedures and documentation requirements**

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

<b>Priv.I.B.1.d.2</b>
-----------------------

version April 1, 2003
-----------------------

## **Business Associate Model Contract Addendum**

On this \_\_\_ day of \_\_\_\_\_, 200\_, the undersigned \_\_\_\_\_ (“Covered Entity”) and \_\_\_\_\_ (“Business Associate”), enter into this Business Associate Contract Addendum (“Addendum”).

**1. Introduction:** Covered Entity is subject to the Standards for Privacy of Individually Identifiable Health Information (45 CFR Parts 160 and 164) (the “Rule”). Covered Entity and Business Associate have entered into a contract more fully described on Exhibit 1(A) (“Contract”). Under the Contract, Business Associate provides, for or on behalf of Covered Entity, the products and/or services described on Exhibit 1(B) (“Covered Services”) and, in the process, receives individually identifiable health information which is protected under the Rule (“PHI”). As a result, Covered Entity and Business Associate enter into this Addendum in order to comply with the Rule, and particularly 45 CFR 164.502.

### **2. Uses and Disclosures of PHI:**

(A) Except as provided in Paragraph 3, Business Associate is permitted and/or required to use and disclose the PHI it obtains pursuant to the Contract and/or in the process of furnishing the Covered Services, only as described in Exhibit 2(A) (“Permitted Uses and Disclosures”). Business Associate is prohibited from any use or disclosure beyond the Permitted Uses and Disclosures without written permission of Covered Entity according to its current policy, a copy of which is available to Business Associate upon request. Business Associate is specifically prohibited from any use or disclosure of the PHI that would violate the requirements of the Rule, if done by the Covered Entity.

(B) Attached hereto and made a part hereof is Covered Entity’s Notice of Privacy Practices as required by 45 CFR §164.520. Business Associate shall comply with any obligations and restrictions on the use, disclosure or request for PHI contained therein that are applicable to it.

### **3. Other Permitted Uses and Disclosures:** Notwithstanding Paragraph 2, Business Associate may use the PHI:

(A) to perform data aggregation services (as permitted by 45 CFR § 164.504(e)(2)(i)(B)) or the creation of a limited data set (as described in and limited by 45 CFR § 164.514(e)) if listed in Exhibit 2(A);

(B) to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1);

(C) for a use that is necessary for the proper management and administration of Business Associate or to carry out its legal responsibilities; and

(D) for a disclosure that is necessary for the proper management and administration of the Business Associate or to carry out its legal responsibilities, but only if:

(i) The disclosure is required by law; or

- (ii) Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

**4. Other Obligations of Business Associate:** In addition to the foregoing, Business Associate shall, with regard to the PHI:

- (A) Not use or further disclose the PHI other than as permitted or required by the Contract (as modified by this Addendum), by the individual as permitted or required by the Rule, or as required by law;
- (B) Use appropriate and commercially reasonable administrative, technical and physical safeguards to prevent use or disclosure of the information other than as provided for by the Contract (as modified by this Addendum);
- (C) Promptly report to Covered Entity any use or disclosure of the information not provided for by the Contract (as modified by this Addendum) of which it becomes aware, have in place procedures to mitigate any harmful effects from the inappropriate use or disclosure, and mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of this Addendum;
- (D) Ensure that any agents, including a subcontractor, to whom it provides the PHI agrees to the same restrictions and conditions that apply to Business Associate with respect to such information;
- (E) In the event of a request by the individual pursuant to the Rule (45 CFR §164.524) for access to PHI in a designated record set in the possession of Business Associate, promptly make the PHI available directly to the individual or to Covered Entity upon request for the purpose of providing access to the individual, according to Covered Entity's current written policy (a copy of which will be made available to Business Associate upon request)<sup>1</sup>;
- (F) In the event of a request by the individual pursuant to the Rule (45 CFR §164.526) to amend PHI in a designated record set in the possession of Business Associate, promptly comply with the applicable provisions of the Rule or make the PHI available to Covered Entity for amendment according to Covered Entity's current written policy (a copy of which will be made available to Business Associate upon request). In the event that the amendment is accepted by Business Associate pursuant to Covered Entity's current written policy, communicate same to Covered Entity. In the event that Covered Entity accepts the amendment, incorporate said amendments to the PHI maintained by Business Associate as required by the Rule<sup>2</sup>;
- (H) Maintain data on all disclosures of PHI for which accounting is required by 45 CFR 164.528 for at least six years after the date of the last such disclosure, and in the event of a request for an accounting of disclosures pursuant to the Rule (45 CFR §164.528), provide the disclosure as required therein or make that data available to Covered Entity according to Covered Entity's current written policy (a copy of which will be made available to Business Associate upon request)<sup>3</sup>;

<sup>1</sup> Alternative: "Promptly make the PHI available to Covered Entity upon request in compliance with the access provisions of the Rule (45 CFR §164.524);"

<sup>2</sup> Alternative: "Promptly make the PHI available for amendment and incorporate any amendments to the PHI maintained by Business Associate as required by the Rule (45 CFR 164.526);"

<sup>3</sup> Alternative: "Promptly make information on disclosures of PHI available to Covered Entity upon request in compliance with the disclosure accounting provisions of the Rule (45 CFR 164.528);"

(I) Provide to Covered Entity promptly upon request such information in Business Associate's possession that is required by Covered Entity to make disclosures required or permitted by law, including but not limited to disclosures required by subpoenas and court orders;

(J) Make its internal practices, books, and records relating to the use and disclosure of the PHI available to the Secretary for purposes of determining the Covered Entity's compliance with the Rule;

(K) At termination of the contract, to the extent feasible, recover all PHI in the possession of its agents and subcontractors and return or destroy all of the PHI that the Business Associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the Contract (as modified by this Addendum) to the remaining PHI and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(L) Remain knowledgeable of the requirements applicable to Business Associates under the Rule and provide appropriate education and training to employees, officers, directors, agents, and contractors to ensure their knowledge of and compliance with those provisions.

#### **5. Obligations of Covered Entity:**

(A) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(B) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

(C) Covered Entity shall notify Business Associate of any change to its Notice of Privacy Practice required by 45 CFR §164.520 that would affect Business Associate's compliance herewith.

**6. Term:** This Addendum shall become effective on April 14, 2003 and, except as hereinafter provided, shall remain in force and effect until the last of the PHI is returned to Covered Entity or destroyed. Notwithstanding the forgoing, the rights and obligations provided by Sections 4(J), 12(B), 12(D), and 4 (to the extent that Business Associate has not returned or destroyed any portion of the PHI) shall survive indefinitely.

**7. Termination of Contract:** Notwithstanding any provision of the Contract to the contrary regarding term or termination, as hereinafter provided Covered Entity is authorized to immediately terminate the Contract if it determines that Business Associate has violated a material term of this Addendum (a "Privacy Breach").

(A) If it is possible to cure the Privacy Breach, upon learning of a Privacy Breach, unless Covered Entity reasonably believes that Business Associate has already cured the Privacy Breach (i.e., has remedied the condition leading to or causing the Privacy Breach), Covered Entity shall give written notice thereof ("Notice") to Business Associate at the address listed on Exhibit 7(A).

(B) If it is not possible to cure the Privacy Breach, or if Covered Entity has not received satisfactory assurances within ten (10) days of the date of the Notice that Business Associate has cured the Privacy Breach, then Covered Entity shall immediately terminate the Contract if, in Covered Entity's sole discretion, it determines that termination is feasible. If Covered Entity determines that termination is not feasible, it shall immediately report the problem to the Secretary of the Department of Health & Human Services.

**8. Conflicting provisions:** In the event that any requirements or provisions of this Addendum should be in conflict with any requirements or provisions of the Contract, the requirements or provisions of this Addendum shall control.

**9. Changes required by law:** The parties hereto have acknowledged that this Addendum is entered into in order to comply with the requirements of the Rule. In the event that the provisions or interpretation of the Rule are materially changed, or in the event that other law is enacted or interpreted which materially effects the terms of this Addendum, the parties agree to enter into a mutually acceptable amendment to this Addendum, on or before the effective date of that change, to bring the terms hereof into compliance therewith.

**10. Compliance with Security Regulations:** In addition to the other provisions of this Addendum, if Business Associate creates, receives, maintains or transmits electronic PHI on Covered Entity's behalf, Business Associate shall, on or before the compliance date for 45 CFR Part 164 Subpart C specific in 45 CFR 164.318:

(A) In addition to Section 4(B), implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of Covered Entity;

(B) In addition to Section 4(D), ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; and

(C) In addition to Section 4(C), report to the covered entity any security incident of which it becomes aware;

**11. Definitions:** As used in this Addendum, the following terms have the following meanings:

“Business Associate” includes not only the person or entity executing this Addendum, but also includes all of its employees, officers, directors, agents, and contractors.

“Disclosure” or “disclose” means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information, as more fully described in the Rule.

“Electronic protected health information” means PHI that is transmitted by electronic media or maintained in electronic media.

“Individual” has the same meaning as the term “individual” in 45 CFR § 164.501 and includes a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

“Security incident” means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

“Use” means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information, as more fully described in the Rule.

## **12. Miscellaneous:**

(A) **Ownership of PHI:** The PHI to which Business Associate has access under the Contract or this Addendum shall be and remain the property of Covered Entity.

(B) Indemnification: Each party to this Addendum shall indemnify and hold the other harmless from any and all liability, damages, costs and expenses, including attorneys fees and costs of defense, resulting from the action or omission of the other party.

(C) Injunctive Relief: Notwithstanding any rights or remedies provided for in this Addendum, Covered Entity retains all rights to seek injunctive relief to prevent or stop the inappropriate use or disclosure of PHI directly or indirectly by Business Associate.

(D) No Third Party Beneficiaries: Nothing in this Addendum is intended to confer upon or create in, nor shall anything herein confer upon or create in, any person other than the parties and their successors and assigns, any rights, remedies, obligations, or liabilities whatsoever.

(E) Choice of Law: This Addendum shall be governed by the laws of the State of Louisiana.

(F) Attorneys Fees: If any legal action or other proceeding is brought for the enforcement of this Addendum or in connection with any of its provisions, the prevailing party shall be entitled to an award for the attorneys fees and costs incurred therein in addition to any other right of recovery.

(G) Amendment: No amendment or other change to this Addendum shall be effective unless reduced to writing and signed by both parties hereto.

(H) Severability: In case any one or more of the provisions contained in this Addendum shall be invalid, illegal, or enforceable in any respect, the validity, legality, and unenforceability of the remaining provisions contained in this Addendum shall not be in any way affected or impaired.

THUS DONE AND SIGNED on the date first written above.

**Witnesses:**

**Covered Entity:**

\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
By: \_\_\_\_\_  
Title: \_\_\_\_\_

**Witnesses:**

**Business Associate:**

\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
By: \_\_\_\_\_  
Title: \_\_\_\_\_

**Business Associate Contract Addendum Exhibits**

1(A) – Description of contract between Covered Entity and Business Associate:

1(B) – Description of Covered Services:

2(A) – Permitted Uses and Disclosures<sup>4</sup>

7(A) – Notices required by this Addendum shall be sent as follows:

**Covered Entity:**

[Name]  
[Institution]  
[Address]  
[City, State Zip Code]

**Business Associate:**

[Name]  
[Institution]  
[Address]  
[City, State Zip Code]

**Copy to:**

[Name]  
[Institution]  
[Address]  
[City, State Zip Code]

**Copy to:**

[Name]  
[Institution]  
[Address]  
[City, State Zip Code]

© Healthcare Provider Management, Inc., 2003  
This document can be reproduced only for the internal compliance use of the purchaser.

<sup>4</sup> “We do not require business associate contracts to identify each disclosure to be made by the business associate....” (Comments, page 82642)

“Rather, the contract must state the purposes for which the business associate may use and disclose protected health information, and must indicate generally the reasons and types of persons to whom the business associate may make further disclosures.” (Preamble, page 82505)

## OCR Discussions on Safeguards

The privacy standards provide, at § 164.530(c), as follows:

- (c) (1) *Standard: safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.
- (2) (i) *Implementation specification: safeguards.* A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.
- (ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

The following have all been collected from official publications, including preamble and comments to the privacy standards and guidance and frequently asked questions issued by the Office of Civil Rights. They, of course, relate to the privacy rules, but are at the very least a relevant starting point for analysis. The original list has been edited for those statements that are relevant to the physical safeguards standards.

\* \* \*

### Examples of safeguard that may not be required:

**Facility restructuring:** “The Department does not consider facility restructuring to be a requirement under this standard.” OCR FAQ ID Number 197 Updated 7/18/2003

**Structural or systems changes:** “The Privacy Rule does not require the following types of structural or systems changes: private rooms, soundproofing of rooms, encryption of wireless or other emergency medical radio communications which can be intercepted by scanners, encryption of telephone systems.” OCR FAQ ID Number 197 Updated 7/18/2003

**Limiting data access in small practices:** “It may not be reasonable for a small, solo practitioner who has largely a paper-based records system to limit access of employees with certain functions to only limited fields in a patient record, while other employees have access to the complete record. In this case, appropriate training of employees may be sufficient.” OCR FAQ ID Number 215 Updated 7/18/2003. *See “For small practice data access” under Suggested Safeguards, below.*

### Suggested Safeguards:

\* \* \*

**For small practice data access:** “In this case, appropriate training of employees may be sufficient.” OCR FAQ ID Number 215 Updated 7/18/2003.

#### **For file cabinets and records rooms:**

Isolating and locking file cabinets or records rooms to minimize access. OCR FAQ ID Number 215 Updated 7/18/2003.

Requiring that **doors** to medical records departments (or to file cabinets housing such records) remain locked and limiting which personnel are authorized to have the key or pass-code. Preamble, page 82561.

Hospitals could ensure that areas housing patient files are supervised or locked.” OCR FAQ ID Number 197 Updated 7/18/2003.

**Passwords:** Providing additional security, such as passwords, on computers maintaining personal information to minimize access. OCR FAQ ID Number 215 Updated 7/18/2003.

\* \* \*

**Cubicles, dividers and other barriers:** Use of cubicles, dividers, shields, curtains, or similar barriers in an area where multiple patient-staff communications routinely occur. For example, a large clinic intake area may reasonably use cubicles or shield-type dividers, rather than separate rooms, or providers could add curtains or screens to areas where discussions often occur between doctors and patients or among professionals treating the patient. OCR FAQ ID Number 197 Updated 7/18/2003.

**Limiting access to computer record fields:** “A hospital with an electronic patient record system may reasonably [configure their record systems to allow access to only certain fields], and therefore, may choose to limit access in this manner to comply with the Privacy Rule.” OCR FAQ ID Number 215 Updated 7/18/2003.

## WASHINGTON UNIVERSITY HIPAA Security Policy #10

### Physical Safeguards Workstation Use

#### 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 physical measures required to protect electronic information systems and related equipment from unauthorized use.

#### Scope of Policy

The scope of this policy is to specify the proper functions to be performed, the manner in which such functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.

#### Policy

##### 1) Compliance with Washington University Computer Use Policy

To ensure that workstations and other computer systems that may be used to send, receive, store or access EPHI are only used in a secure and legitimate manner, Workforce members who, and workstations and other computer systems that are used to, send, receive, store and access EPHI must comply with the Washington University Computer Use Policy, a copy of which is attached hereto as Exhibit A.

##### 2) WU Monitoring of Workstation Use

Workforce members that use Washington University information systems and workstation assets should have no expectation of privacy. To appropriately manage its information system assets and enforce appropriate security measures, Washington University may log, review, or monitor any data (EPHI and non-EPHI) stored or transmitted on its information system assets.

##### 3) Removal of Workforce Members Privileges

Washington University may remove or deactivate any Workforce member's user privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.

**Creation Date:** January 15, 2004

**Effective Date:** April 14, 2004

**Last Revision Date:** January 21, 2004

## Exhibit A

### WU Computer Use Policy

#### **Introduction**

This document provides guidelines for appropriate use of computer facilities and services at Washington University. It is not a comprehensive document covering all aspects of computer use. It offers principles to help guide members of the Washington University community, and specific policy statements that serve as a reference points. It will be modified as new questions and situations arise.

While the proliferation of computers and information technologies does not alter basic codes of behavior in academic life, it does place some issues in new contexts. Using these technologies enables people to do varied things—both good and bad—more easily. They are an enormously rich resource for innovation in the furtherance of Washington University's academic mission. They also offer new forums for the University's historic commitment to the expression and discussion of a wide diversity of ideas and opinions. But they increase the risks of actions, deliberate or not, that are harmful in various ways, including: (a) interference with the rights of others; (b) violation of the law; (c) interference with the mission of the University; or (d) endangering the integrity of the University's information computer network. The guidelines that follow in the next section of this document seek to forge the link between established codes of conduct and use of new technologies. Computer networking has greatly expanded our ability to access and exchange information, requiring more vigilant efforts and perhaps more secure safeguards to protect individuals' rights of privacy. Property as well as privacy rights may be infringed whenever files or data belonging to others, however gained, are used without authorization; moreover, while freedom of inquiry and expression are fundamental principles of academic life, assaults upon the personal integrity of individual members of the academic community and dissemination of offensive materials may undermine the foundations of that community. Other actions taken by individuals may, under some circumstances, jeopardize the integrity of the computer network and the ability of others to communicate using this system. Accordingly, the guidelines that follow seek to both preserve the freedom to inquire and share information and sustain the security and integrity of individuals within the community and the computer system itself.

While some of the guidelines therefore call for respectful and responsible use of the computer networks to protect the rights of individuals, others warn against actions that may violate the law: users within the academic community must understand the perils of illegal use, exchange, or display of copyrighted, deceptive, defamatory, or obscene materials on a web page or through other electronic communication channels.

The community at large has rights and expectations that must be considered. When individuals misrepresent either themselves or the University, or when they act by computer in a manner unacceptable within the University or in the larger community, the integrity and mission of the University itself is endangered. Finally, the guidelines seek to protect the integrity of the University information systems themselves: the computing or networking resources need to be accessible and secure for appropriate uses consistent with the mission of the University; the usurpation of these resources for personal gain or without authorization is unacceptable. Moreover, even the individual right to privacy may, when personal files may need to be accessed for troubleshooting purposes, be overridden by authorized personnel to protect the integrity of the University's computer systems.

#### **Principles and Guidelines**

##### **A. Respect the rights and sensibilities of others**

1. Electronic mail should adhere to the same standards of conduct as any other form of mail. Respect others you contact electronically by avoiding distasteful, inflammatory, harassing or otherwise unacceptable comments. (In

an academic community, the free and open exchange of ideas and viewpoints preserved by the concept of academic freedom may sometimes prove distasteful, disturbing or offensive to some. This policy is not intended to restrict such exchange.)

2. Others have a right to know who is contacting them.

3. Respect the privacy of others and their accounts. Do not access or intercept files or data of others without permission. Do not use the password of others or access files under false identity.

4. Distribution of excessive amounts of unsolicited mail is inappropriate.

5. While the University encourages respect for the rights and sensibilities of others, it cannot protect individuals against the existence or receipt of materials that may be offensive to them. Those who make use of electronic communications may come across or be recipients of material they find offensive or simply annoying.

#### **B. Be aware of the legal implications of your computer use.**

1. The Internet enables users to disseminate material worldwide. Thus the impact of dissemination on the internet is often far broader than that of a statement made on paper or in routine conversation. Keep in mind that a larger audience means a greater likelihood that someone may object with or without legal basis.

2. Much of what appears on the internet is protected by copyright law regardless of whether the copyright is expressly noted. Users should generally assume that material is copyrighted unless they know otherwise and not copy or disseminate copyrighted material without permission. Copyright protection also applies to much software, which is often licensed to the University with specific limitations on its use. Both individual users and the University may, in some circumstances, be held legally responsible for violations of copyright.

3. Many other state and federal laws, including those prohibiting deceptive advertising, use of others' trademarks, defamation, violations of privacy, and obscenity apply to network-based communications.

4. Because the internet is international, it can be argued that the (often more restrictive) laws of other countries may apply. This does not mean that members of the University community should be censored by extremely restrictive foreign laws, but in some situations the University must take into consideration whether violations of foreign laws may affect the activities of the University in those countries.

#### **C. Respect the mission of the University in the larger community**

1. The University makes internet resources available to students, faculty and staff to further the University's educational, research, medical, service and related missions. While incidental personal use is permissible in most settings, these resources are generally available only for University-related activities.

2. The University does not monitor the content of web pages, electronic mail or other on-line communications and is not responsible for the views expressed by individual users. Under certain circumstances, however, the University may be held liable if it fails to take reasonable remedial steps after it learns of illegal uses of its computer facilities. Use computer resources lawfully.

3. Remember that you are responsible for all activity involving your account. Keep your account secure and private. Do not use identifying data or common words as a password; your password should be difficult to crack or otherwise guess either by individuals or by sophisticated computer programs.

4. The University is the custodian of a wide array of personal and financial data concerning its students, staff, faculty and patients, as well as the University itself. Respect the University obligations of confidentiality as well as your own. Only those with authorization may access, communicate or use confidential information.

5. Material posted on WEB pages is generally accessible and thus deserves even greater thought and care than your private electronic mail. Remember that, absent restrictions, your web page is available to anyone, anywhere, and act accordingly.

6. The university has a right to expect that computer users will properly identify themselves. Computer accounts are assigned and identified to individuals. Don't misrepresent yourself.

#### **D. Do not harm the integrity of the University's computer systems and networks.**

1. Today's information technology is a shared resource. Respect the needs of others when using computer and network resources. Do not tamper with facilities and avoid any actions that interfere with the normal operations of computers, networks, and facilities.

2. Avoid excessive use of computer resources. They are finite and others deserve their share. Chain mail, junk mail, and similar inappropriate uses of University resources are not acceptable. Web pages that are accessed to an excessive degree can be a drain on computer resources and, except where significant to the University's

mission, may require the University to ask that they be moved to a private Internet provider.

3. Although a respect for privacy is fundamental to the University's policies, understand that almost any information can in principle be read or copied; that some user information is maintained in system logs as a part of responsible computer system maintenance; that the University must reserve the right to examine computer files, and that, in rare circumstances, the University may be compelled by law or policy to examine even personal and confidential information maintained on University computing facilities.

4. You are granted privileges and responsibilities with your account. While these vary between groups, the use of University resources for personal commercial gain or for partisan political purposes (not including the expression of personal political views, debate and the like) is inappropriate and possibly illegal.

5. Individual University computer systems have varying resources and demands. Some have additional and sometimes more restrictive guidelines applicable to their own user.

### Implementation

A. All University codes of conduct apply to information technology as well as to other forms of communication and activity.

B. Systems managers or other individuals within an academic or administrative unit may be empowered to suspend some or all privileges associated with computer use in cases of misuse or threat to the integrity of all or part of the University's information management resources.

C. Before any permanent action is taken against a user, the user will be advised of the bases for the proposed action and given an opportunity to respond. Concerns about such actions may be raised through the usual administrative or academic channels associated with the department, school, facility or resource in question.

D. Where a violation of University policies or applicable law appears to warrant action beyond a suspension or elimination of computer privileges, the matter may be referred to a supervisor, administrator or University disciplinary body with appropriate authority or to law enforcement authorities.

E. Complaints or concerns about another's use of University computer resources should be directed to the administrator responsible for the facility or resource in question.

*Approved, Washington University Faculty Senate, May 1997.*

For questions about this policy, contact your school, department, or unit system manager or send e-mail to [Shirley K. Baker](#), Vice Chancellor for Information Technology.

## WASHINGTON UNIVERSITY HIPAA Security Policy #11

### Physical Safeguards Server, Desktop and Wireless Computer System Security

#### 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 physical safeguards that will apply to hardware that may be used to access, transmit, store or receive EPHI.

#### Scope of Policy

The scope of this policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store EPHI to ensure that appropriate security is maintained and that access is restricted to authorized users. Each workstation that is used to access, transmit, receive or store EPHI must comply with each of the aforementioned measures. If any of the aforementioned measures are not supported by the workstation operating system or system architecture, one of the following steps must be taken:

- The server, desktop computer system, or wireless computer system must be upgraded to support all of the following security measures
- An alternative security measure must be implemented and documented
- The workstation must not be used to send, receive or store EPHI.

#### Policy

##### 1) Server Security Requirements

- a) Each Business Unit must ensure that all servers used to access, transmit, receive or store EPHI are appropriately secured in accordance with this Policy.
- b) Servers must be located in a physically secure environment. (See [HIPAA Security Policy #9- Facility Access Control](#)).
- c) The system administrator or root account must be password protected. (See [HIPAA Security Policy #13- Access Control](#)).
- d) A user identification and password authentication mechanism must be implemented to control user access to the system. (See [HIPAA Security Policy #13- Access Control](#)).
- e) A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
- f) Servers must be located on a secure network with firewall protection. If for any reason the server must be maintained on a network that is not secure, an intrusion detection system must be implemented on the server to detect changes in operating and file system integrity. (See [HIPAA Security Policy #13-Access Control](#)).

- e) All unused or unnecessary services shall be disabled.

## 2) Desktop System Security Requirements

- a) Each Business Unit must ensure that each desktop system used to access, transmit, receive or store EPHI is appropriately secured in accordance with this Policy.
- b) The system administrator or root account must be password protected. (See [HIPAA Security Policy #13 - Access Control](#)).
- c) A user identification and password authentication mechanism must be implemented to control user access to the system. (See [HIPAA Security Policy #13 - Access Control](#))
- d) A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
- e) A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up to date.
- f) All unused or unnecessary services must be disabled.
- g) Desktop systems that are located in open, common, or otherwise insecure areas must also implement the following measures:
  - An inactivity timer or automatic logoff mechanisms must be implemented. (See [HIPAA Security Policy #13 - Access Control](#)).
  - The workstation screen or display must be situated in a manner that prohibits unauthorized viewing. The use of a screen guard or privacy screen is recommended.

## 3) Mobile Systems Security Policy

- a) Each Business Unit must ensure that all mobile systems used by Workforce Members to access, transmit, receive or store EPHI are appropriately secured in accordance with this Policy.
- b) The system administrator or root account must be password protected. (See [HIPAA Security Policy #13 - Access Control](#)).
- c) A user identification and password authentication mechanism must be implemented to control user access to the system. All mobile devices and laptops must use a boot password to ensure that the system is only accessible to authorized users. (See [HIPAA Security Policy #13 - Access Control](#)).
- d) A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
- e) A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up-to-date.
- f) All unused or unnecessary services must be disabled.
- g) Mobile stations that are located or used in open, common, or otherwise insecure areas must also

implement the following measures:

- A theft deterrent device such as a laptop locking cable must be utilized when the device is unattended.
- An inactivity timer or automatic logoff mechanism must be implemented. (See HIPAA Security Policy #13 - Access Control).
- Reasonable safeguards must be in place prohibit unauthorized entities from viewing confidential information such as logins, passwords, or PHI.

h) Personal Digital Assistants (PDAs) and other handheld mobile devices must not be used for long-term storage of EPHI. EPHI stored on hand held mobile devices must be purged as soon as it is no longer needed on that device, with a storage time not to exceed 30 days.

i) Each mobile system that is used to access, transmit, receive, or store EPHI must comply with as many of the aforementioned measures as is allowed by the system and operating system architecture.

**Creation Date: January 15, 2004**

**Effective Date: April 14, 2004**

**Last Revision Date January 21, 2004**

## WASHINGTON UNIVERSITY HIPAA Security Policy #12

### Physical Safeguards Device and Media Controls

#### 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 ensure that the receipt and removal of hardware and electronic media containing EPHI complies with the Security Regulations.

#### Scope of Policy

The scope of this policy is to outline the policy and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility and the movement of such items within the facility.

#### Policy

##### 1) General Application of Policy

- a) These policies and procedures pertain to the use of hard drives, storage systems, removable disks, floppy drives, CD ROMs, PCMCIA cards, memory sticks, and all other forms of removable media and storage devices.
- b) The procedures developed pursuant to this Policy must be documented and submitted to the HIPAA Security Office for approval.

##### 2) Destruction of Storage Devices or Removable Media

- a) Prior to destroying or disposing of any storage device or removable media, care must be taken to ensure that the device or media does not contain EPHI.
- b) If the device or media contains the only copy of EPHI that is required or needed, a retrievable copy of the EPHI must be made prior to disposal.
- c) If the device or media contains EPHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal. A typical reformat is not sufficient as it does not overwrite the data.

##### 3) Reuse of Storage Devices or Removable Media

- a) Prior to making storage devices and removable media available for reuse, care must be taken to ensure that the device or media does not contain EPHI.
- b) If the device or media contains the only copy of EPHI that is required or needed, a retrievable copy of the EPHI must be made prior to reuse.
- c) If the device or media contains EPHI that is not required or needed, and is not a unique copy, a data

destruction tool must be used to destroy the data on the device or media prior to reuse. A typical reformat is not sufficient as it does not overwrite the data.

d) 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, the use of a data destruction tool between uses is not necessary.

#### **4) Movement of Equipment Housing EPHI**

a) Each Business Unit shall develop a procedure to determine when an exact retrievable copy of EPHI is required prior to the movement of equipment storing such EPHI.

b) When using storage devices and removable media to transport EPHI each Business Unit must develop a procedure to track and maintain records of the movement of such devices and the media and the parties responsible for the device and media during its movement.

**Creation Date: January 15, 2004**

**Effective Date: April 14, 2004**

**Last Revision Date: January 21, 2004**

**WASHINGTON UNIVERSITY**  
**Draft HIPAA Security Policy #12.2.1 (1)**

**Physical Safeguards**  
**Facility Access Control Policy**

**Policy Provisions:** To ensure that access to facilities used to house EPHI-based systems is appropriately controlled the following procedures must be established and implemented:

- Each Business Unit must create and maintain a Facility Security Plan that outlines and documents the procedures to safeguard all facilities, systems, and equipment used to store EPHI against unauthorized physical access, tampering, or theft. The Facility Security Plan must include the following components:
  - o Contingency Operations – procedures that allow physical facility access during emergencies to support restoration of data under a Disaster Recovery Plan. (See HIPAA Security Policy # 7 - Contingency Planning)
  - o Access Control and Validation – procedures to control and validate a workforce member’s access to facilities based on their role or function.
  - o Physical Access Records – procedures to log physical access to any facility containing medium and high risk EPHI-based systems. Examples of facilities requiring physical access records are computer and system rooms.
  - o Maintenance Records – procedures to document and manage repairs and modifications to the physical security components of the facility including locks, doors, and other physical access control hardware.
- Procedures must be established and implemented to control and validate workforce member access to all facilities used to house EPHI based systems.
  - o All workforce members must wear their University Identification Badges at all times when on campus.
  - o A physical access control mechanism must be utilized to control physical access to all facilities containing EPHI-based systems. Code locks, badge readers, and key locks are examples of physical access control mechanisms.
- Procedures must be established and implemented to control, validate, and document visitor access to any facility used to house EPHI based systems. This procedure applies to vendors, repair personnel, or other non-workforce members.
  - o All visitors requiring access to facilities containing EPHI-based systems must sign in providing information regarding their identity and the purpose of their visit.
  - o All visitors must be provided a temporary identification badge or be escorted to and from their destination.

This policy includes, but is not limited to, the aforementioned procedures. The sub-policies and procedures defined in this policy must be reviewed and evaluated on a periodic basis to ensure that they maintain their 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 24, 2003

**Date of Last Edit:** January 22, 2004

**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](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](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](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](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](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](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](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](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](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](http://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://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://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://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  
19<sup>th</sup> 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](http://www.NSP.cc)

**Travis Planchard, CEO**

[tplanhard@nsp.cc](mailto:tplanhard@nsp.cc)

Office - 225.709.2591

Fax - 225.709.2592