Washington University in St. Louis
School of Medicine
Department of Radiation Oncology

HIPAA Security Procedure #1
General Security Compliance

Last Revised: 1/21/2004	*Effective date: 4/14/2004*

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 its compliance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the security of Electronic Protected Health Information ("EPHI")(the "Security Regulations").

Scope of Policy

The scope of this Policy covers Washington University's general approach to compliance with the Security Regulations. As a covered entity under the Security Regulations, WU must: (1) ensure the confidentiality, integrity and availability of all EPHI WU creates, receives, maintains or transmits; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and (4) ensure compliance with the Security Regulations by its Workforce. Compliance with the Security Regulations will require WU to implement:

- Administrative Safeguards--those actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect EPHI and to manage the conduct of WU's Workforce in relation to the protection of and authorized access to said EPHI.
- Physical Safeguards--those physical measures, policies and procedures to protect WU's electronic information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
- Technical Safeguards--the technologies and the policies and procedures for its use that protect EPHI and control access to it.

The specifications for implementation of each of these safeguards are addressed in three separate sets of policies. The Administrative Safeguards are set forth in HIPAA Security Policies #1 through 8; the Physical Safeguards are set forth in HIPAA Security Policies #9 through 12; and the Technical Safeguards are set forth in HIPAA Security Policies #13 through 17.

Policy

1) A Hybrid Entity

Washington University is a hybrid entity under the Security Regulations with both covered and noncovered functions. WU hereby designations its HIPAA covered functions as health care components for purposes of the Security Regulations. WU's health care components are set forth in Exhibit A, attached hereto and incorporated herein, which Exhibit may be revised from time to time. Included within each designated health care component are various support services including, without limitation, legal, accounting, audit, finance, tax, risk management, information systems management, maintenance, facilities, environmental health and safety and the University's Compliance Office. Individuals who perform such support services for both HIPAA health care components and non-covered functions shall not use Protected Health Information that they obtain in the course of furnishing services for the HIPAA covered health care components to provide services to the non-covered functions. In addition, when Using or Disclosing Protected Health Information, the HIPAA covered health care components shall treat the non-covered functions as if they were legally separate entities. References within the Washington University HIPAA Security Policies to Washington University or WU mean the HIPAA covered entity components of Washington University.

2) A Single Affiliated Covered Entity

WU has ownership or membership interests in a number of separate legal organizations. These separate legal organizations shall be considered a single affiliated covered entity with Washington University for purposes of the Security Regulations, and shall be included as part of the Washington University School of Medicine ("WUSM") HIPAA health care component of WU. The separate legal entities that will be included as part of the WUSM component part of WU are set forth on Exhibit B, attached hereto and incorporated herein, which Exhibit may be revised from time to time.

3) An Organized Health Care Arrangement

WUSM and its affiliated teaching hospitals, Barnes-Jewish Hospital ("BJH") and St. Louis Children's Hospital ("SLCH"), participate in a clinically integrated care setting in which patients typically receive health care services from employees and agents of each of WUSM, BJH and SLCH. WUSM, BJH and SLCH have designated themselves as an organized health care arrangement and it is anticipated that each of BJH, SLCH and WUSM will coordinate their respective implementation of the Security Regulations. Except as specifically stated herein or as might be agreed to in writing, each of BJH, SLCH and WUSM shall be responsible for ensuring its own compliance with the Security Regulations and in no event shall any of them be responsible for any other party's failure to comply with the Security Regulations.

4) Security Personnel and Implementation

On behalf of its covered entity component parts, WU has designated a Security Officer with overall responsibility for the development and implementation of policies that conform to the Security Regulations ("Security Policies"). The initial HIPAA Security Officer is Paul Schoening, HIPAA Security Officer, Associate Dean for Academic Information Management, and Director of the Medical Library. The Security Officer has identified a number of Business Units within the HIPAA covered entity components of WU. Each Business Unit has named a HIPAA Security Liaison. The Business Unit HIPAA Security Liaison is responsible for ensuring that the Business Unit: (i) complies with the HIPAA Security Policies, (ii) develops and implements business-unit specific HIPAA security procedures ("Security Procedures") for each Security Policy that is applicable to that Business Unit, (iii) maintains the confidentiality of all EPHI created or received by the Business Unit from the date such information is created or received until it is destroyed, and (iv) trains all Workforce members within the Business Unit at the appropriate level of HIPAA training as determined by the HIPAA Security Officer.

The Security Regulations permit WU to implement any security measure that allows it to reasonably and appropriately comply with a specific security standard in the Security Regulations. In determining which security measures to implement, WU must take in to account its size, complexity and capabilities; technical infrastructure; hardware and software security capabilities; the costs of the security measures; and the probability and criticality of potential risks to EPHI. In the Security Policies, WU has determined that Business Units in some cases *must* implement a particular security measure and in other cases have *discretion* to determine which security measures to implement. In those cases in which a Security Policy permits a Business Unit to exercises discretion in the implementation of a security measure, the Business Unit must notify and obtain the prior approval of the Security Officer for the measure implemented so that WU may ensure that it complies with the Security Regulations.

5) Security Complaints

The Security Officer shall be responsible for facilitating a process of individuals to file a complaint regarding WU's Security Policies or the handling of EPHI by a WU HIPAA health care component. The Security Officer shall be responsible for ensuring that the complaint and its disposition are appropriately documented and handled.

6) Mitigation, Sanctions and Non-Retaliation

WU shall ensure that its HIPAA health care components mitigate damages for any violation of the Security Regulations and the WU Security Policies and/or Security Procedures, appropriate discipline and sanction employees and other Workforce members for any violation, and refrain from intimidating or retaliating against any person for exercising his or her rights under the Security Regulations or for reporting any concern, issue or practice that such person believes in good faith to be in violation of the Security Regulations or the WU Security Policies and/or Security Procedures. WU shall not require any persons to inappropriately waive any rights of such person to file a complaint with the Department of Health and Human Services.

7) Security Policies and Procedures

The WU HIPAA Security Policies and Security Procedures are designed to ensure compliance with the Security Regulations. Such Security Policies and Security Procedures shall be kept current and in compliance with any changes in the law, regulations or practices of WU's covered entity component parts in accordance with HIPAA Security Policy #8 - Periodic Evaluation of Security Policies and Procedures.

8) Responsibility of All Employees within WU HIPAA Covered Entity Component Parts

Every member of the WU Workforce within a HIPAA covered entity component part of WU is responsible for being aware of, and complying with, the Security Regulations and the Security Policies and Security Procedures.

EXHIBIT A

COMPONENT PARTS

1. Health Care Provider Component Parts

a) Washington University School of Medicine ("WUSM") (including the Barnes-Jewish Hospital Dialysis Center, Farmington Dialysis Center, Chromalloy American Kidney Center);

b) Psychological Counseling Service of the Department of Psychology in the School of Arts and Sciences

c) Student Health and Counseling Services

2. Health Plan Component Parts

a) Washington University Comprehensive Employee Welfare Benefit Plan (including medical plans, flexible health spending account plan and the employee assistance plan)

b) Health Plan for Washington University undergraduates

c) Health Plan for Washington University Post-Doctoral Fellows

d) Health Plan for Washington University School of Medicine students

EXHIBIT B

AFFILIATED ENTITIES

Washington University Pain Control, L.L.C.
Cardiothoracic Surgery North, LLC
Washington University Physician Network
Washington University Physician Network d/b/a Barnes Eyecare Network
The Heart Care Institute, LLC
Heart Care Institute Affiliated Services, LLC
Washington University Health Ventures, Inc.