TO OUR VISITORS

Welcome to the Department of Radiation Oncology at Washington University School of Medicine. We hope you find your stay with us to be educational and rewarding. Please take a few minutes to read the material below regarding our policies and procedures on Protected Health Information.

- All computer and paper databases must be registered, using the Database Registration Form.
- Please complete the Confidentiality Form.
- Please read the attached information on HIPAA so that you are aware of our policies and procedures regarding protecting health information (PHI).

WHEN YOU LEAVE

- PHI may not be removed from the premises when your visit ends. Contact your sponsor if you wish to discuss ways in which PHI can be de-identified.
- You must remove or destroy all PHI of any kind, whether paper or electronic, which you may have created while a visitor with us.
- PHI should be disposed of by shredding the data, clearing the hard drive, destroying diskettes, stripping data of all identifiers, etc.
- A visiting resident leaving the Medical Center cannot take PHI. Residents may take de-identified, aggregate data only.

DEPARTMENT OF RADIATION ONCOLOGY
WASHINGTON UNIVERSITY SCHOOL OF MEDICINE
POLICIES AND PROCEDURES
HIPAA

HIPAA stands for the Health Insurance Portability and Accountability Act. This law, passed by Congress in 1996, protects an individual's right to health coverage during events such as changing or losing jobs, pregnancy, moving, or divorce. It also provides rights and protections for employers when getting and renewing health coverage for their employees.

HIPAA imposes certain requirements on health providers and health plans regarding the confidentiality of patient health information and the disclosure of such patient health information to third parties.

We may not use or disclose PHI unless:

- it is for treatment, payment or health care operations
- the individual specifically authorizes the use or disclosure in writing
- the use or disclosure is permitted or required by law

We have a duty to protect patient health information every day and in every way. This includes health information that is spoken, written and electronic.

What is Protected Health Information (PHI)?

PHI is any health information by which an individual patient can be identified. PHI may exist in written, electronic, oral or any other form. This includes past, present or future physical or mental health. The 19 data elements of PHI are:

(1) Name or initials
(2) Street address, city, county, precinct, zip code and equivalent geocodes
(3) All elements of dates (except year) for dates directly related to an individual and all ages over 89
(4) Telephone number
(5) Fax number
(6) Electronic mail address
(7) Social Security Number

(8) Medical record numbers
(9) Health plan ID numbers
(10) Account numbers
(11) Certificate/license numbers
(12) Vehicle identifiers and serial numbers, including license plate numbers
(13) Device identifiers and serial numbers
(14) Web addresses (URLs)
(15) Internet IP addresses
(16) Biometric identifiers, including finger and voice prints
(17) Full face photographic images and any comparable images
(18) Any other unique identifying number, characteristic or code
(19) Patient initials

Giving out any unauthorized patient information in any form is both unethical and illegal. It is our duty under HIPAA to put safeguards in place to protect patient privacy. If we don't, we could be charged with criminal and civil penalties. It's the law.

9 Tips are:

1. Prevent malicious software or viruses from corrupting information.

   This means that downloading things from the Internet could bring viruses into your computer, which could cause you to lose patient information or to disclose it to others when it isn't appropriate. Many Internet screen savers, games and downloads contain viruses.

2. Protect patient health information when it leaves the facility.

   What if the files were taken, not signed out, and not returned? If that patient or the patient's physician needed the information, it would not be available, and that's illegal. What if the person taking it dropped the files and the contents blew down the street? That is not keeping the patient's files confidential.

3. Practice good password management.

   The reason everyone is given a computer password is so the information that they use is kept confidential. Your password should be shared with no one else. It should not be posted in a place where others could find it. Your password should not be easy for someone else to figure out, and it should be changed frequently.

4. Secure workstations, including printers, faxes and computers.

   Do not leave patient information where others can see it. That means faxes, computer monitors, printers, etc should be in a secure location where patients and other workers are not constantly passing by.

5. Dispose of patient health information appropriately.

   You cannot leave medical records in a regular trash can where anyone could pull them out and read them. Any medical records are to be destroyed properly.

6. Always wear your ID badge.

   It doesn't matter if you see patients every day. If you work here, you should wear your ID badge where it can be read. It shouldn't be turned around backwards, worn at your waist or on a low pocket and your name should be visible.

7. Close doors, cabinets, file drawers, and keep desk clean and put files away.

   You cannot leave medical records sitting out in the open. Patient private medical information should be locked up when you are not present to guard it. Do not leave notes sitting out on your desk "Call Mrs. Smith about her pregnancy". This is private health information.

   When you are talking to a patient, or about a patient, make reasonably sure that others cannot hear your voice, especially those who do not have a need to know the information.

8. Restrict oral communication.

   Do not discuss patient information in public. This includes elevators, hallways, cafeterias or other public places.

9. Restrict access and disclosure of patient health information.

   Patient health information should only be available on a "need to know" basis. You wouldn't like people who don't know you and who are not involved in your health care to be discussing your condition.

Remember, HIPAA is the law. Keeping this information confidential is everyone's responsibility.

When you leave Washington University

1. PHI may not be removed from the premises when your visit ends. Contact your sponsor if you wish to discuss ways in which PHI can be de-identified.

2. You must remove or destroy all PHI of any kind, whether paper or electronic, which you may have created while a visitor with us.

3. PHI should be disposed of by shredding the data, clearing the hard drive, destroying diskettes, stripping data of all identifiers, etc.

4. A visiting resident leaving the Medical Center cannot take PHI. Residents may take de-identified, aggregate data only.

For Additional Information or Questions

Privacy Liaison – WUSM Radiation Oncology
Kevin Sharkey
Tel 314-286-1076
FAX 314-362-8521
Campus Box 8224
ksharkey@radonc.wustl.edu

or

University Privacy Office
HIPAA@msnotes.wustl.edu
Tel 314-747-4975

Security Liaison – WUSM Radiation Oncology
Chris Alexander
Tel 314-362-9741
FAX 314-362-9797
Campus Box 8224
calexander@radonc.wustl.edu

HIPAA Contact - BJH
David Ray
Medical Records
Tel 314-362-1913

Web Sites

1. WUSM HIPAA web site, http://hipaa.wustl.edu
2. HSC web site, http://medicine.wustl.edu/~hsc/

Glossary of HIPAA Terms

Business Associate means a person or entity who (1) on behalf of a covered entity performs or assists in a function or activity involving the Use or Disclosure of Individually Identifiable Health Information, including claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; repricing; and other functions and activities; or (2) provides legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation or financial services that involves the disclosure of Individually Identifiable Health Information.

Business Unit means one or more Workforce members who are subject to the HIPAA regulations and who are engaged in providing a specific product or service that involves Protected Health Information on behalf of the Covered Entity. (As applied to the University, a business unit may be a department, a program or school, a support service or central administration function within the University. A business unit may extend across multiple locations.)

Correctional Institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Covered Entity means entities to which the HIPAA rules apply and includes Health Plans, Health Care Clearinghouses and Health Care Providers who transmit any health information in electronic form in connection with a Transaction covered by HIPAA laws and regulations. Washington University is a Covered Entity.

De-identified Health Information means health information that is not individually identifiable health information. A covered entity may determine that health information is not individually identifiable health information only if: (1) a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk is very small that the information could be used, alone or in combination with other available information, to identify an individual, and documents the methods and results of the analysis; or (2) the following identifiers of the individual, relatives, employers or household members of the individual are removed:

(1) Name;
(2) Street address, city, county, precinct, zip code and equivalent geocodes;
(3) All elements of dates (except year) for dates directly related to an individual and all ages over 89;
(4) Telephone number;
(5) Fax number;
(6) Electronic mail address;
(7) Social Security Number;
(8) Medical record numbers;
(9) Health plan ID numbers;
(10) Account numbers
(11) Certificate/license numbers;
(12) Vehicle identifiers and serial numbers, including license plate numbers;
(13) Device identifiers and serial numbers
(14) Web addresses (URLs);
(15) Internet IP addresses;
(16) Biometric identifiers, including finger and voice prints;
(17) Full face photographic images and any comparable images; and
(18) Any other unique identifying number, characteristic or code.

Designated Record Set means medical records and billing records that are used to make decisions about individuals and are maintained by or for a Health Care Provider. It also means the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a Health Plan. The term record means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a Covered Entity such as Washington University.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. Therefore, Disclosure is to parties external to Washington University.

Group Health Plan (not to be confused with the St. Louis managed care plan of the same name) means an employee welfare benefit plan (as defined by ERISA) or insured and self-insured plans that provides medical care (as defined by the Public Health Service Act) to employees or their dependents directly or through insurance that:

(1) Has 50 or more participants (as defined by ERISA); or
(2) Is administered by an entity other than the employer that established and maintains the plan. See related definition for Health Plan.

Health Care means care, services, or supplies related to the health of an individual and includes, but is not limited to, the following:

> (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
> (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that do either of the following functions:

> (I) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
> (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Operations means any of the following activities carried out directly by Washington University or through an Organized Health Care Arrangement in which Washington University participates:

> (I) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
> (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of Health Care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities.

(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);
(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
(6) Business management and general administrative activities including, but not limited to:

(I) Management activities relating to implementation of and compliance with the requirements of HIPAA laws and regulations;
(ii) Customer service, including the provision of data analyses for policyholders, plan sponsors, or other customers,
provided that Protected Health Information is not disclosed to such policyholder, plan sponsor, or customer.
(iii) Resolution of internal grievances;
(iv) Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a Covered Entity or, following completion of the sale or transfer, will become a Covered Entity; and
(v) Creating de-identified health information, fundraising for the benefit of Washington University, and marketing for which an individual authorization is not required as described by HIPAA laws and regulations.

Health Care Provider means a provider of medical or health services and any other person or organization that furnishes, bills for, or is paid for health care in the normal course of business (generally, facilities and health care providers as defined for Medicare purposes).

Health Insurance Issuer means an insurance company, insurance service, or insurance organization that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a Group Health Plan. See related definitions for Group Health Plan and Health Plan.

Health Oversight Agency means an agency or other governmental authority, including employees, agents or contractors of such agency or authority, authorized by law to oversee the health care system (whether public or private) or government programs in which PHI is necessary to determine eligibility or compliance or to enforce civil rights law. For example, the federal Centers for Medicare and Medicaid (a.k.a. Health Care Financing Administration), JCAHO and the Missouri Department of Health.

Health Plan means an individual or group plan that provides or pays the cost of medical care and includes the following, singly or in combination:

(1) A Group Health Plan, as defined herein
(2) A Health Insurance Issuer, as defined herein
(3) An HMO, as defined herein
(4) Part A or Part B of the Medicare program under Title XVIII
(5) The Medicaid program under Title XIX
(6) An issuer or a Medicare supplemental policy
(7) An issuer or a long-term care policy, excluding a nursing home fixed-indemnity policy
(8) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers
(9) The health care program for active military personnel under title 10 of the United States Code
(10) The veterans health care program under 38 U.S.C. chapter 17.
(11) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)
(12) The Indian Health Service program under the Indian Health Care Improvement Act
(13) The Federal Employees Health Benefits Program
(14) An approved State child health plan under Title XXI providing benefits for child health assistance
(15) The Medicare + Choice program under Part C of Title XVIII
(16) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals
(17) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care

Individual means the person who is the subject of Protected Health Information.

Individually Identifiable Health Information is information that is a subset of health information, including demographic information collected from an individual, and:

(I) Is created or received by a Health Care Provider, Health Plan, employer, or Health Care Clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of Health Care to an Individual; or the past, present, or future payment for the provision of Health Care to

an Individual; and
(A) Identifies the Individual; or
(B) reasonably could be used to identify the Individual.

Law Enforcement Official is an officer or employee of any agency or authority of the United States, a State or territory, political subdivision of a State or territory, or Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law or prosecute or otherwise conduct criminal, civil or administrative proceeding arising from an alleged violation of law.

Limited Data Set is Protected Health Information that excludes the following identifiers of the Individual, or of relatives, employers or household members of the Individual: names, postal address information other than town or city, state and zip code, telephone numbers, fax numbers, electronic mail address, social security number, health plan beneficiary number, account number, certificate/license number, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers, web universal resource locators (URLs), Internet Protocol (IP) address numbers, biometric identifiers, including finger and voice prints and full face photographic images and any comparable images.

Marketing means to make a communication about a product or service to encourage recipients of the communication to purchase or use the product or service. Communications are not considered marketing when they are:

(1) a face-to-face communication made by a Covered Entity to an individual;
(2) a promotional gift of nominal value provided by the Covered Entity;
(3) for the purpose of describing the entities participating in a Health Care Provider network or Health Plan network, or for the purpose of describing if and the extent to which a product or service (or payment for such) is provided by a Covered Entity or included in a plan of benefits;
(4) for treatment of the Individual or
(5) for case management or care coordination for that individual or to direct or recommend alternative treatments, therapies, health care providers or settings of care to that individual.

Minimum Necessary is a term that applies when Washington University Uses, Discloses or requests Protected Health Information other than for Treatment purposes. The amount of Protected Health Information shared among the internal or external parties shall be the minimum amount necessary to accomplish the purpose of the Use or Disclosure. For internal Use, the amount of information necessary to accomplish the purpose varies by job title or job classification.

Organized Health Care Arrangement means:

(I) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
(2) An organized system of health care in which more than one Covered Entity such as Washington University participates, and in which the participating Covered Entities:

(A) Hold themselves out to the public as participating in a joint arrangement; and
(B) Participate in joint activities that include at least one of the following:

(i) Utilization review, in which Health Care decisions by participating Covered Entities are reviewed by other participating Covered Entities or by a third party on their behalf;
(ii) Quality assessment and improvement activities, in which treatment provided by participating Covered Entities is assessed by other participating Covered Entities or by a third party on their behalf; or
(iii) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating Covered Entities through the joint arrangement and if Protected Health Information created or received by a Covered Entity is reviewed by other participating Covered Entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A Group Health Plan and one or more such plans each of which are maintained by the same plan sponsor; or
(4) The Group Health Plans described in paragraph (3) of this definition and Health Insurance Issuers or HMOs with respect to such group health plan but only with respect to Protected Health Information created or received by such health insurance issuers and HMOs plans that relates to Individuals who are or have been participants or beneficiaries in any of such Group Health Plans.

Payment means the activities undertaken by a Health Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the Health Plan or undertaken by a Health Care Provider or Health Plan to obtain or provide reimbursement for the provision of health care that relate to the Individual to whom Health Care is provided. Example activities include, but are not limited to:

(1) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
(2) Risk adjusting amounts due based on enrollee health status and demographic characteristics;
(3) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related Health Care data processing;
(4) Review of health care services with respect to medical necessity, coverage under a Health Plan, appropriateness of care, or justification of charges;
(5) Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and
(6) Disclosure to consumer reporting agencies of any of the following Protected Health Information relating to collection of premiums or reimbursement:

(A) Name and address;
(B) Date of birth;
(C) Social security number;
(D) Payment history;
(E) Account number; and
(F) Name and address of the Health Care Provider and/or Health Plan.

Protected Health Information means Individually Identifiable Health Information that is transmitted by electronic media; maintained in any electronic media; or transmitted or maintained in any other form or medium. Protected health information excludes Individually Identifiable Health Information in education records covered by the Family Educational Right and Privacy Act.

Psychotherapy Notes means notes recorded (in any medium) by a Health Care Provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy Notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public Health Authority means an agency or authority of the United States, a State, territory, political subdivision of a State or territory, Indian tribe, person or entity acting under a grant of authority from or contract with such public agency including the employees or agents of such public agency, its contractors or delegated persons that is responsible for public health matters as part of its official mandate.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to Health Care. It includes the following types of information
transmissions:

(1) Health care claims or equivalent encounter information
(2) Health care payment and remittance advice
(3) Coordination of benefits
(4) Health Care claim status
(5) Enrollment and disenrollment in a Health Plan
(6) Eligibility for a Health Plan
(7) Health Plan premium payments
(8) Referral certification and authorization
(9) First report of injury
(10) Health claims attachments
(11) Other transactions that the Secretary may prescribe by regulation

Treatment means the provision, coordination, or management of health care and related services by one or more Health Care Providers, including the coordination or management of health care by a Health Care Provider with a third party; consultation

between Health Care Providers relating to a patient; or the referral of a patient for Health Care from one Health Care Provider to another.

Use means, with respect to Individually Identifiable Health Information, the internal sharing, employment, application, utilization, examination, or analysis of such information maintained by Washington University

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Washington University, is under the direct control of Washington University whether or not they are paid by Washington University.