Washington University in St. Louis

HIPAA Privacy Procedure #1

Effective Date: April 14. 2003
Reviewed Date: February, 2011
Revised Date: February, 2011
Scope: Radiation Oncology

Accountabilities for Compliance to HIPAA Privacy Rules

****

Policy Expectation:
Washington University (WU) is committed to conducting business in compliance with all applicable laws, regulations and WU policies related to HIPAA. The policy to which this procedure relates introduces the relationship among WU, BJH, SLCH and other institutions within BJC Healthcare and outlines the component parts of WU that are subject to the HIPAA privacy rules.

Why is this important?
This procedure describes general principles and actions to be taken to allocate and ensure accountability toward such commitment.

Failure to comply may result in WU being liable for civil and criminal penalties under the HIPAA regulations.

What do you need:
1. HIPAA Privacy Policy #1, Privacy Compliance
2. HIPAA Glossary of Terms
3. OHCA – organized health care arrangement – is between WUSM, BJH and SLCH.

Steps:	Additional Information
1. Adopt a philosophy to ensure compliance with HIPAA rules: • Inform Individuals of privacy rights and how Protected Health Information (PHI) will be Used and Disclosed by WU. • Adapt generic procedural templates and know how the HIPAA privacy rules apply.	See Radiation Oncology HIPAA Procedure, #12, Distribution of Notice of Privacy Practices. See approved Radiation Oncology Privacy Procedures on the HIPAA web site. Procedures are also posted on Department Policy shared computer drive accessible to all radiation oncology employees and also on the Rad Onc OCF website http://ocf.wustl.edu/Hipaa/

• Train the Workforce in an understanding of HIPAA privacy rules.	Each new employee (staff, faculty, part time, full time, temporary) is seen by Lisa DeBerry in Dept Personnel/Payroll Office. They complete a Confidentiality Form and a Database Registration Form. Lisa DeBerry notifies Kevin Sharkey, Privacy Liaison, of last four digits of their social security number. Privacy Liaison obtains password and sends notice to new employee of requirement for HIPAA training. Level of training is based on job classification. Privacy Liaison follows up to ensure training is completed through periodic training reports received from WU Privacy Office. All faculty and staff are asked to self-report to the Privacy Liaison on an annual basis that they have read each department procedure by turning in a personal training log.
• Designate persons responsible for seeing that privacy procedures are adopted and followed.	As a condition of employment, the supervisor is responsible for ensuring University procedure is followed.
• Secure PHI so that it is not readily available to those who do not need to see it.	Each data repository has an assigned custodian. Two-key computer passwords or two physical keys protect repositories in department.

Do not interrupt, influence or jeopardize patient care with HIPAA rules interpretation or application. Do not prohibit the legitimate Use or Disclosure of PHI. Exercise the Golden Rule: Treat information about others, as you would want others to treat information about you.	
2. Appoint the following groups or persons to ensure compliance with HIPAA rules within each WU Business Unit. • Business Unit Stakeholder Group with persons representing at least research, teaching, clinical financial and administrative aspects of the Business Unit. • Appoint one or more HIPAA Privacy Liaisons to be held accountable for compliance to HIPAA policies and procedures. • Appoint one or more HIPAA Trainers to be held accountable for the orientation of new personnel and the ongoing awareness of existing Workforce members related to HIPAA.	RO Stakeholder Group consists of: ➢ Kevin Sharkey – Privacy Liaison (286-1076) ➢ Walter Bosch – Physics Research (747-5414) ➢ Joseph Deasy – Bioinformatics and Outcomes Research (362-8610) ➢ Robert Drzymala – Clinical Physics (454-5021) ➢ Angel Medina – Business Office (362-9701) ➢ Dan Mullen – Bioinformatics and Outcomes Research (362 - 8534) ➢ Christopher Alexander – Security Liaison (362-9741) ➢ Dr. Wade Thorstad – Radiation Oncologist (362-8516) Kevin Sharkey – Privacy Liaison (286-1076) Kevin Sharkey – Privacy Liaison (286-1076)

• Appoint one or more Security Liaisons to be held accountable for the implementation and compliance with minimum standards related to HIPAA security measures. a. Customize HIPAA Procedure Templates and submit procedures to the Privacy Office for approval and posting on the HIPAA web site. b. Never guess. When in doubt, direct all questions regarding HIPAA to the following persons in sequence listed: • Privacy Liaison / Security Liaison • Privacy Officer/Security Officer	Chris Alexander – Security Liaison (362-9741) The following are Security Stakeholders: ➢ Chris Alexander – Security Liaison (747-9741) ➢ Walter Bosch – Physics Research (747-5414) All procedures for Radiation Oncology are available at any time on the HIPAA web site. Kevin Sharkey Privacy Liaison (286-1076) Chris Alexander Security Liaison (362-9741)
3. Change the way sensitive information is communicated: • Be able to demonstrate that reasonable steps are taken to protect the privacy of PHI. • Be sensitive to patient needs; err on the side of being conservative. • Be sensitive to patient wishes about sharing his/her PHI with friends and family. • Avoid unintended sharing of PHI by conversation in any location, while using answering machines, making announcements in patient waiting areas, and when using clip boards, white boards, view boxes, chart holders and computer screens. • Observe precautions in locating and using a fax machine.	See Radiation Oncology HIPAA Procedures, located on the HIPAA web site. Procedures are also posted on Department Policy Shared computer drive and on the Rad Onc OCF website http://ocf.wustl.edu/Hipaa/ which is accessible to all radiation oncology employees

4. Create procedural steps to ensure the privacy and security of clinical and research data in electronic, film, specimen and paper formats.	
• Define where PHI resides in any format, how it moves into and out of the prescribed safe location, who decides how it is Used, Disclosed, stored and destroyed and the criteria for making such decisions.	See Procedure #17-2 on data repositories and Procedure #15 on research.
• Clearly define the components of the Designated Record Set and account for the safe maintenance of any data retained in a separate location within the physical file or location.	See approved procedures on HIPAA web site.
• Designate a time period, accountability for and monitoring of timely filing of all data into clinical and research records.	Filing of material into research records should be completed by designated employee in the workgroup on timely basis.
• Designate a custodian (plus back-up) for each record location.	Each repository has a named custodian of record with the Privacy Liaison. Each custodian of a high-risk database has designated a secondary representative to act in the custodian's absence.
• Verify the identity of everyone who enters a record location.	Procedure #17-2
• Know if the requesting party needs the records for Treatment, Payment or Healthcare Operations.	Procedure #17-2
• Keep track of records when they leave the designated safe location.	Procedure #17-2
• Do not release anything to an outside party without appropriate authorization or procedure.	See Procedure #5 Authorization Required; Procedure #11 Minimum Necessary Disclosure; Procedure #13 Disclosures without Authorization; Procedure #15 Research.
• Track the release of PHI to show compliance with HIPAA privacy rules.	Exhibit A, Tracking Tool for Custodians of PHI.

• Provide for safe destruction of hard copy data through the location of and access to shredders. • Provide physical security through the "2-key" principle, use of out guides and use of criteria for taking records out of the safe location and off premises.	Shred boxes are located in all areas: 4 CSRB; lower level CAM; Forest Park. Blanket purchase orders have been given to 2 vendors for shredding. 1 vendor does on-site shredding. Shred certificates are kept in department business office for 6 years.
• Register and annually re-register all electronic and spreadsheet databases.	See Procedure #17-2 on repositories.
5. Participate in the University-wide effort to address complaints related to HIPAA procedures. • Refer all complaints to the Privacy Office. • Participate in research and resolution of any complaint as directed by the Privacy Office and in the time frame specified. • Expect to see internal sanctions for violations of privacy such as: a. Disclosure of PHI by trained staff to other members of the Workforce who are not trained in the WU HIPAA procedures, and b. Use or Disclosure of PHI inappropriately for personal or malicious reasons.	Refer to the HIPAA Procedure, #12 for a description of the complaint process. Refer to the WU Code of Conduct for more detail on sanctions ranging from disciplinary action to termination related to violations of HIPAA procedures.
6. Design and provide appropriate training and retraining of the WU Workforce. • Establish a method for becoming aware of the arrival of new faculty, staff, students, visiting professors and other similar categories of persons present in the Business Unit.	See #1 above. Sponsors in department of all visitors are to comply with department procedure on Visitors. This procedure is filed on Dept Policy drive.

• Assign levels and content of training required based on the job functions of each member of the WU Workforce.	See #1 above. Also Procedure #11 Minimum Necessary.
• Define a training schedule within each Business Unit. Include non-Workforce members such as rotating students, visiting professors, observers, temporary agency workers and visitors other than professors.	Training shall occur prior to any exposure to any PHI and prior to gaining access to systems like IDX. All faculty and staff are trained with HIPAA training web site. Department continues to educate faculty and staff in dept procedures through Exhibit B Personal Training Log.
7. Initiate HIPAA training within the first week on WU premises.	
• Make training a requirement for access to any computer system or database.	See #1 above.
• Include in the general HIPAA training specific instructions on how to execute the procedures customized for the Business Unit.	For persons on the premises for one month or less, written certification of general HIPAA training obtained at another location will be honored. However, exposure to Radiation Oncology specific procedures (via the Rad Onc HIPAA Visitor's Packet) is required along with signature on a Confidentiality Statement. Privacy Liaison verifies completion of required training.
• Develop methods to monitor completion of training.	Instructions on how to access web-based training are filed on Dept policy drive.
• Impress the importance and severity of penalties of non-compliance.	By letter from department chairman to faculty and staff and visitors.

8. Establish a decentralized monitoring process to ensure HIPAA Compliance. • Monitoring is done for compliance by internal and external parties. • All employees are responsible for compliance through "management by walking around" to observe the following actions as representative of possible HIPAA privacy violations. a. PHI in trash cans. b. Observation of conversations among staff. c. Visibility of PHI on computer screens, work surfaces and other similar informational display areas. d. Locks not locked. e. Public access to fax machines, chart racks. f. Passwords and usernames posted for access by multiple parties. g. Inappropriate destruction of data on hard drives and discs and in sold or discarded furniture and equipment. h. Work areas housing PHI left unattended during work hours and unsecured after hours.	Non-compliant disclosures, discovered in audit or reported by employee or discovered through daily work observance, will be reported by employee involved to Privacy Liaison using a paper version of Exhibit C, Electronic Disclosure Log. Paper form will be given to Privacy Liaison who will enter in web site Electronic Disclosure Log. The paper copy will be retained on file for 6 years**.**
• Designate one or more action steps to ensure the procedure will be/is being followed. • Follow the rule of thumb used for documentation: "If it isn't documented, it did not happen" and convert it into "If we cannot prove compliance to HIPAA procedures, it did not happen."	The objective is to show compliance with any rule established. "If we say it in procedural print, can we prove it in action?" Privacy liaison will review all multi-user databases yearly, to review disclosures and access procedures. Single user or paper databases will be reviewed on random basis. A written record will be kept of audit results. (e.g., check on 2 key security, etc.)

EXHIBIT A

HIPAA Tracking Tool for Custodians of PHI

(Electronic or Medical Records)
[Not to be used for Patient Access - See Procedure #2]

Date of Request:_____

Department of Person Requesting PHI:_____

Method of Identity of Person Requesting PHI:

ID Badge:_____
Other (specify):_____

Covered Entity Affiliation:

WU_____ BJH_____ SLCH_____

Other:_____
(Must be Accounted Patient)

==========

Patient Name:_____ MRN or SSN_____
or
Data List:_____

What is being requested:_____

Purpose of Request:_____

==========

Treatment, Payment of Healthcare Operation (TPO)
Permitted/Required - Reference Policy and Procedure #13

Note Type of Disclosure:_____

Research
No IRB Action

Research Preparatory to Research (No information can be copied or removed)
Research on Decedent

With IRB Authorization Letter: Compliant with:
Authorization - Full Access (attach copy)
Limited Data Set - Dates/Zip Codes (attach copy)
*Waiver - Full Access (attach copy)

==========

Show compliance to the HIPAA Minimum Necessary Rule by describing PHI release

Entire designated Record set:

Medical Record
Billing Record
Portions of designated record (specify below)

Electronic Records (specify)_____

_____

_____

Number of Records Released (attach a list if available)_____

==========

Requesting Party Signature_____

PHI Custodian Signature_____

Date of Release_____

EXHIBIT B PERSONAL TRAINING LOG

To: Kevin Sharkey
HIPAA Privacy Liaison
Department of Radiation Oncology

The following verifies that I have reviewed all Department procedures relating to HIPAA Federal regulations.

_____ _____
Printed Name Signature

Procedure No.	Procedure Name	Date Reviewed	Your Initials
01	Accountabilities for Compliance		
02	Access by Individuals to PHI		
03	Accounting for Disclosures of PHI		
04	Amendment of PHI		
05	Authorization Required for Uses or Disclosures of PHI		
06	Use or Disclosure with Business Associates		
07	Appropriate Methods of Communicating PHI		
08	Use or Disclosure in Fundraising		
09	Use or Disclosure in Marketing		
10	Use or Disclosure in Media Relations		
11	Minimum Necessary Request		
12	Distribution of Privacy Practices		
13	Uses or Disclosures without Verbal or Written Authority		
14	Use or Disclosure of Psychotherapy Notes		
15	Use of Disclosure in Research		
16	Requests for Restrictions and Alternative Methods for Communication		
17-2	Identification of Repositories		
17-3	Access to Electronic PHI		
17-4	Passwords		
17-6	Electronic Sharing/Transmission of Data Containing PHI		
17-7	Communication by E-Mail		
18	Verbal/Inferred Agreements		

On Department Policies Computer Drive Under

HIPAA Forms

Procedure No.	Policy Name	Date Reviewed	Your Initials
None	PHI 19 Elements		
None	Research Definitions		
None	HIPAA Visitor Training Packet		
None	Who to Call		
None	Contact Person		
None	Form: Request for Access to Records		
None	Faculty and Residents When You Leave		

Exhibit C Accounting of Disclosures of Protected Health Information

Staff Information

Department:	Radiation Oncology
Phone Number:	
Email:	
Position:	
Other Position :	

Patient Information

Patient First Name:			
Patient Last Name:			
Date of Birth:	Month	Day	Year
SSN:			
MRN:			
Patient Disclosure:			

Person or Entity Receiving Information

Person or Entity Name:	
Identity Verified by:	
Identity Verified by Other:	
Street:	
City:	
State:	
Zip:	

Disclosed Information

Disclosed Date:	Month	Day	Year			
Disclosed Information:						
Date/Date Range of Information Disclosed:	Month	Day	Year	Month	Day	Year
Purpose of the disclosure:						