Washington University in St. Louis

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

HIPAA Privacy Procedure #17-2

Repositories with Protected Health Information

****

Policy Expectation:

Electronic repositories of Protected Health Information (PHI) shall be protected in accordance with all applicable laws, rules, regulations and department policies. Electronic repositories are considered databases, defined as any collection of information maintained electronically or in paper form or on disk or on tape, and are to be documented and maintained by persons appointed as custodians by the Department of Radiation Oncology.

Why is this important?

- Ensure that the existence and location of all electronic repositories of PHI are known.
- Facilitate responding to Individuals who exercise the right of an accounting of certain Uses or Disclosures of PHI.
- Facilitate the assignment of access rights and passwords to the repository.
- Failure to comply may result in being liable for civil and criminal penalties under the HIPAA regulations.

What do you need:

- Copy of the HIPAA Policy on Security Measures Required to Comply with Privacy Policies.
- Cost Sheet for making records available to Individuals.
- Database Registration Form
- HSC web site, http://medicine.wustl.edu/~hsc/
- WU HIPAA website, http://hipaa.wustl.edu

Steps:	**Additional Information**
1. The Database Registration form will be presented to each new employee along with the Confidentiality Agreement, at time of New Employee Orientation in the department. A copy of the completed form will be given to RO Privacy Liaison and to the RO Security Liaison. The RO Privacy Liaison will retain form on file for 6 years.	Database Registration Form Exhibit A can be accessed on Department Drive,

2. The RO Security Liaison will review all database registration forms received and will designate database level of risk (low or high).	RO Privacy Liaison Kevin Sharkey Tel 314-286-1076 FAX 314-362-8521 Campus Box 8224 mailto:ksharkey@radonc.wustl.edu
3. The Database Registration form will be presented to each visitor to the department by the faculty sponsor arranging the visit. Form will be presented for completion, along with the Confidentiality Form, and the HIPAA Training Information and the HIPAA Receipt of Training Form. Completed forms are to be submitted to RO Privacy Liaison, along with the completed Confidentiality Form, who will retain on file for 6 years.	RO Security Liaison Chris Alexander Tel 314-362-9741 FAX 314-362-9797 Campus Box 8224 calexander@radonc.wustl.edu
4. Each repository/database has a named custodian on record, who is responsible for overall security for that repository, and who authorizes access by others to the repository. Access may be partial or total.	
5. Each custodian will designate a secondary representative in the event the custodian is not available to comply with a request from the RO Privacy Liaison.	No secondary representative will be appointed for low risk databases. A secondary representative will be named for high-risk databases.
6. Custodians of data repositories (electronic or physical) containing PHI should register their data repository with the ROC Privacy Liaison. a. All data repositories, electronic or paper, which contain PHI, must be registered annually by custodians of those repositories. If your repository contains any of the categories of identifiers at the bottom of the Database Registration form, you need to register the database. b. Custodian is the person who owns or manages access to a data repository. c. If you have more than one database on a computer but the data is all managed in the same way, register all data as one repository. For example, if Dr. XX has 2 databases and clinical notes on his CAM desktop, but he is the only user to access all this data, he could register: Description: "Dr XX clinical repository", Custodian: "Dr XX"	

Location: Dr XX CAM desktop, D drive. If, however, one of the databases is a lung study that 3 physicians access, Dr. XX should register the lung study separately. d. Databases that you use but do not manage (e.g. Clinical Desktop) need NOT be registered by you. The Custodian of that database will register it and manage your access (examples: Departmental Mail Server, Tumor Registry, IDX, RAPID) e. Password Management Method: Describe physical or electronic keys. (e.g. locked office, locked suite, computer login/password, database password) f. If you are not the Custodian for any repositories of data containing PHI, sign and date the 2nd signature line, "I am not the Custodian..." and return to RO Privacy Liaison.	
7. Register your data repository with the HSC using Form 24 (if necessary)	
8. Enforce a two key password (or physical key) policy for your repository. a. One key can be "Secure Network" if repository resides there b. One key can be "User Authentication", user/password for domain c. One key can be "Locked Office" when you are not physically there.	
9. Enforce proper permission for access to your repository. a. Document your repository registration and access administration for review by departmental, university or Federal HIPAA authorities. b. Assign an Assistant Custodian who can access your repository documentation in your absence. c. File the name of your Assistant Custodian with the ROC Privacy Liaison.	
10. Document permissions (account access or physical access) you grant for repository use: a. Job-related: (Treating MD, Nurse, Billing Specialist, etc.) Keep a hard copy of each request for account or access. b. Preparatory to research: Keep documentation that the	

researcher provides. c. Subject Recruitment: Keep a copy of the HSC study approval letter. d. HSC Authorization: Keep a copy of the HSC approval letter. e. Departmental Authorization: Keep a copy of the authorization (For instance, Permission to keep PHI in a treatment database for the purpose of recruitment for future research studies). f. HSC Waiver of Authorization (Full or Partial): Keep a copy of the HSC Waiver. g. Data Use Agreement (DUA - using limited data set): You, the custodian, can sign an agreement with the data requestor concerning use of only the fields described as the limited data set. (See the DUA form on the HSC website). Keep a copy of the DUA. h. Code Access Agreement (CAA): the material shared contains none of the patient identifiers except a re-identification code. The CAA is usually used with a lab (internal or external to WU), which processes tissue samples. Check with the HSC for proper filing. Keep a copy of the CAA for your records. i. Other confidentiality agreement: The HSC may create confidentiality agreements for sharing PHI or modify existing agreements.	See Privacy Policy #15
11. Track disclosures of PHI that are subject to accounting. Disclosures are subject to accounting if the disclosure relates to: ▪ Research conducted under a Waiver ▪ Preparation for research ▪ Decedent Research Record the following: a) Reason for Disclosure (Waiver, Prep for Research, Decedent) b) To whom/Time period/Study name and purpose	
12. Respond to Requests for Accounting	
13. Respond to each notification of patient revocation of authorization. a. Document and time stamp the notification of revocation of authorization. b. Notify the users of your repository who are affected by this revocation. (For instance, the revocation could be limited to a particular study or a particular field. The revocation does not apply to data already disclosed, but it	

does apply to future disclosures.) c. Adapt your repository data to prevent future disclosures/use of patient data addressed by the revocation.	

14. To Request data from a data repository: ▪ Formulate a Research Question ▪ Register with the database or repository custodian ▪ Give data repository custodian a copy of your HSC Approval letter describing protocol or research activity type and level of permission ▪ Give data repository custodian a copy of your HSC Waiver Letter describing protocol or research activity type and level of permission ▪ Give data repository custodian your identification: visitor, WU employee or notification of new job duty assignment requiring additional access (e.g. member of research team for HSC study) ▪ DUA (data use agreement): Sign a DUA with the database or repository custodian for use of limited data set fields for a specific purpose (a DUA does not need HSC approval) ▪ Other permission agreement (other agreements may be devised by the HSC for approved legal use of data containing PHI).	See Privacy Policy #3
15. A treating MD can maintain a repository/database of patients treated. The MD is custodian and must register the repository/database with the ROC. Privacy Liaison. The treating MD might refer to the database for treatment decisions, may formulate a research question from the database and may recruit from patients in the database without documentation. But a research study will require HSC consent and an approval letter. When other researchers use the database, the documentation of the appropriate permission must be maintained.	
16. Records are to be maintained for 6 years from latest date records were accessed.	
17. PHI used in research should be disposed of properly by shredding the data, clearing the hard drive, destroying diskettes, strip data of all identifiers, etc.	
18. The Radiation Oncology Privacy Liaison shall annually review Repository forms that are on file and remove and shred forms that are greater than 6 years old.	
19. The RO Privacy Liaison will conduct an annual audit to determine that custodians are in compliance with applicable policies and this procedure.	See Exhibit A

Exhibit A
Annual Registration of Repositories/Databases

Definition of Repository/Database = any collection of information maintained electronically or in paper form.

This form will be retained on file for audit/accounting purposes for 6 years.

Repository/Databases Containing Identifiable Protected Health Information (Any of the *19 Identifiers)

Repository/Database Title	Custodian	# of Users Who Access	Password Managed Method	Approx. # of Patients in Repository/ Database	Location	RO Privacy Liason Date Reviewed	RO Privacy Liason Initials

I understand the duties entrusted to me as a Custodian of the above repository/database(s) and agree to maintain the repository/database according to Washington University and Federal guidelines.

_____ _____ _____

Signature of Database Custodian | Date | Printed Name of Database Custodian

I am not the Custodian of any repository/database(s) containing Protected Health Information as determined by Washington University and Federal guidelines.

_____ _____ _____

Signature | Date | Printed Name

RETURN THIS FORM (IN HARD COPY) TO Kevin Sharkey (CAMPUS BOX 8224) RADIATION ONCOLOGY HIPAA LIAISON/TRAINER. ALSO, PLEASE KEEP A COPY FOR YOUR RECORDS

* 1. Name
2. Street address, 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 (URL's)
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's initials