University of Minnesota
Center for Magnetic Resonance Research
Policy
Protected Health Information (PHI)

Policy Number / Version: POL009 / Version 1
Approval Date: 01/16/2015
Implementation Date: 01/16/2015
Author/Owner: Brian Hanna / John Strupp

Approval Signatures	**Date**
Author/Owner:	
Regulatory Compliance Coordinator:	
Center Director:	

1. Purpose

The purpose of this policy is to define the safeguarding electronic Protected Health Information (PHI) at the CMRR. This policy details CMRR standard operating policy/procedure and is compatible with all applicable regulatory, IRB, University Security and Privacy office, and AHC policies. Please notify the author if any inconsistencies are found.

2. Scope

This policy will apply to all researchers conducting research at CMRR that includes PHI.

3. Definitions

- PHI is protected health information, as defined by applicable IRB and University policies.
- Researcher refers to any individual using CMRR facilities.
- Staff refers to any CMRR employee.

4. Responsibility

It is the responsibility of all personnel who perform the functions listed in Section 2 to adhere to this policy.

It is the responsibility of the owner/author listed above to review the content of this policy for accuracy and continued applicability on at least an annual basis.

5. Policy

At a minimum, PHI includes the following:

1. Name
2. All geographic subdivisions smaller than a state (street address, city, county, precinct) Note: you can retain the first 3 digits if the zip code area contains more than 20,000 people.
3. For dates directly related to the individual, all elements of dates, except year (date of birth, admission date, discharge date, date of death).
4. All ages over 89 or dates indicating such an age, except that you may have an aggregate category of individuals 90 and older.
5. Telephone number
6. Fax number
7. Email address
8. Social security number
9. Medical record number
10. Health plan number
11. Account numbers
12. Certificate or license numbers
13. Vehicle identification/serial numbers, including license plate numbers
14. Device identification/serial numbers
15. Universal resource locators
16. Internet protocol addresses
17. Biometric identifiers, including finger and voice prints
18. Full face photographs and comparable images
19. Any other unique identifying number, characteristic or code.

PHI stored on paper (Consent forms)

PHI written on paper, such as consent forms, should be managed by the researcher according to the relevant University policies. See below.

No PHI stored on CMRR magnet scanners, computers, servers, or systems

No PHI is to be entered into the magnet scanner systems or patient registration screens.

No PHI is entered into or stored on any CMRR computers or servers.

No PHI is entered into any CMRR calendar or billing system.

No PHI is to be stored on any CMRR system.

Any exceptions to this policy must be documented in an approved ePHI data plan.

ePHI Data Plans

An ePHI data plan includes the exact location and data processing steps for all electronic PHI in use. These plans must be reviewed and updated on a yearly basis by the researcher. These plans are approved by designated CMRR PHI technical staff and maintained for review by the IRB and the University Data Protection office.

PARS Applications

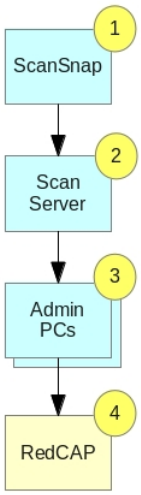
The PARS application will contain a checkbox about electronic PHI and a way for researchers to upload an ePHI plan.

Limited PHI Collected for IRB reporting

PHI for research volunteers is written onto paper forms as each volunteer registers and visits for a scan. These are scanned into the network scanner (1) by the researcher and automatically sent to the scan server (2). The paper forms are retained by the researcher. Each researcher is responsible to maintain those records in accordance to HIPAA and IRB guidelines.

Scans on the scan server (2) are retained for a period of two months and then deleted.

These PHI scans are viewed on administrative PCs (3) and the data keyed into the UMN RedCap database. The scans are attached during entry and uploaded into RedCap. (4) No PHI is stored on the administrative PCs (3).



No PHI is entered into any calendar or billing system. An accession number (sequential event number) from Imagecast is entered into some calendar entries to help tie calendar events to Imagecast scans.

Removal of PHI Access on Termination

Staff members will surrender all keys and cards on termination to the CMRR lab manager Jeramy Kulesa.

Access to the CMRR Active Directory (Windows PC) computers will be terminated by Andy Berhow (CMRR Computer Resource Group).

Access to the RedCap PHI database, the CMRR servers, and calendar/project databases will be terminated by Brian Hanna (CMRR Computer Resource Group).

In the case of non-voluntary termination, appropriate and timely steps will be taken to terminate access regardless of the cooperation of the terminated individual.

6. References

For details on what data is allowed and how to de-identify data, refer to the University policy and procedure documents on PHI.

HIPPA policy:
http://www.policy.umn.edu/Policies/Operations/Health/HIPAACOMPONENT.html
De-Identifying PHI:
http://www.policy.umn.edu/Policies/Operations/Health/HIPAACOMPONENT_PROC11.html
De-Identifying PHI for research:
http://www.policy.umn.edu/Policies/Operations/Health/HIPAARESEARCH_PROC04.html

7. Appendices / Tables

N/A

8. Revision History

Version Number	Approval Date	Change from Previous Version