Statement of Policy

It is the policy of Purdue’s Regenstrief Center for Healthcare Engineering (RCHE) that all employees who have been designated as covered by HIPAA are responsible for maintaining the confidentiality and security of patient health information. Special protections exist for Protected Health Information (PHI), and this policy specifies appropriate procedures and security to be used by RCHE staff to safeguard this information. All RCHE PHI is defined in the RCHE Designated Record Set.

This policy applies to the individually identifiable health records that are accessed or maintained by RCHE and protected by HIPAA. The policy is consistent with existing University handling requirements and HIPAA compliance policies.

Reason for Policy

RCHE has established this compliance policy to ensure that all staff, faculty and researchers involved with identifiable health records are properly informed. This policy shall serve as a guideline for the handling of data, security and the appointment of those to administer HIPAA related documentation.

HIPAA Liaison

The HIPAA liaison is responsible for the implementation and maintenance of HIPAA resources and compliance. The role of the liaison is of utmost importance in ensuring that the HIPAA regulations are followed in each of the covered entities at Purdue. Good communication and coordination with the Director of HIPAA Privacy Compliance is necessary to ensure that procedures are up-to-date with changes and regulations and that issues and questions are resolved expeditiously.

The liaison is to act as the primary point of contact for questions, audits, training and communication. The liaison is also responsible for identifying others to administer duties as required. RCHE’s HIPAA liaison is Ken Musselman, kenmus@purdue.edu. A detailed description and list of responsibilities can be found at: http://www.purdue.edu/hipaa/secondary_menu/administration/liaisons/liaisonexpectations.pdf

Individuals and Entities Affected by Policy

RCHE workforce who are designated as covered by HIPAA and assigned a particular project are affected by this policy. All staff are required to know this policy and abide by the confidentiality described. Inappropriate use or disclosure of individually identifiable health information shall be reported to the RCHE HIPAA Liaison or the Director of HIPAA Privacy Compliance. The University may apply sanctions to employees who violate HIPAA policies and procedures.
Who Should Know Policy

RCHE staff and researchers may encounter health information protected by HIPAA through various sources including but not limited to interoffice communications, data, electronic media, verbal interactions, etc. All RCHE staff and researchers who have access to PHI, storage areas of information or involvement with projects that make use of PHI shall know the HIPAA policy and shall sign a confidentiality agreement.

Exclusions

RCHE workforce whose space is within RCHE, but do not have access to PHI, storage areas of PHI information or involvement with a project that makes use of PHI are excluded from signing the confidentiality agreement.

Website Address for Policy

Policy is located on the RCHE website: www.purdue.edu/rche
University HIPAA related information and forms can be found at: www.purdue.edu/hipaa

Definitions

HIPAA = Health Insurance Portability Accountability Act of 1996

Individually Identified Health Information = Information that is a subset of health information, including demographic information collected from an individual. This information is created or received by a healthcare provider, health plan or employer and relates to past, present or future condition of an individual.

Protected Health Information (PHI) = all individually identifiable health information that is a subset of health information, including:
- demographic information collected from an individual
- is created or received by a covered health care provider, health plan, employer or health care clearinghouse; and
- relates to the past, present or future physical or mental health or condition of an individual
- the provision of health care to an individual
- the past, present or future payment for the provision of health care to an individual that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual

Designated Record Set = data which contains individually identifiable data, in any medium, accessed or maintained for RCHE. The content may be in multiple locations and media, including paper and electronic form.
**Limited Data Set** = PHI that excludes the following identifiers of the individual, individual’s 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 addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- 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
- Full face photographic images and any comparable images

**De-identified Data Set** = PHI that excludes the following identifiers of the individual, individual’s relatives, employers or household members of the individual:

- Names
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- 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
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code

**Responsibilities**

All RCHE employees who have been designated as covered by HIPAA are responsible for maintaining the confidentiality and security of PHI. This applies to PHI that are accessed or maintained by RCHE and are protected by HIPAA and is consistent with university handling requirements. All RCHE staff are responsible for the safety of information.

The HIPAA liaison shall be responsible for determining that the appropriate workforce members have access to the necessary PHI and that the required security processes are in place. The liaison shall also be responsible for implementing procedures to terminate access to HIPAA protected information and the storage of this information.

**Documentation**

RCHE is required to implement policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications or other requirements of HIPAA. These policies and procedures take into account the size and the type of activities that relate to PHI undertaken by RCHE, to ensure such compliance.

Documentation shall include at a minimum:
1. policies and procedures shall be maintained in written or electronic form
2. any communications shall be in written or electronic form
3. if an action, activity or designation is required to be documented, a written or electronic copy shall be maintained

**Training**

RCHE is responsible to ensure that all its employees, new or existing, are trained regarding the HIPAA regulations and its privacy policies and procedures. Training includes but is not limited to:
- HIPAA training – on-line or with HIPAA training officer (certificate of completion required)
- CITI (test scores and verification required)
- HIPAA communication guidelines
- Confidentiality Agreement (must be signed)

Follow-up to ensure compliance shall be done annually. All certifications and paperwork shall be maintained by the RCHE HIPAA Liaison or assigned designee.
IT Administration

RCHE, a HIPAA-designated Purdue covered component as of August 1, 2010, is responsible for maintaining the confidentiality and security of project-specific provider and patient health information. The center conducts applied research to determine how to practically and effectively improve healthcare delivery and to develop areas of knowledge for future healthcare engineering advancements. The projects seek to be multi-disciplinary in nature and can span a number of collaborating universities. The Protected Health Information (PHI) acquired in support of these projects is made available to researchers in accordance with Purdue’s Internal Review Board (IRB) and in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The servers housing this PHI are managed by RCHE and maintained by Information Technology at Purdue (ITaP) on Purdue’s HIPAA-compliant servers. These databases are made available to researchers through user-registered, password-protected accounts or on-line “hub” applications, such as CatalyzeCare.org, that support the project team’s specific collaboration, analysis and development needs.

IT Administrative Functions

Project PI
- Shall be HIPAA certified.
- Shall maintain current list of project researchers who have access to the project data.
- Shall notify the Data Manager of the researchers who shall have access to the above data.
- Shall audit researchers’ use of the data throughout the project to ensure minimum necessary access and proper compliance with Purdue’s Regenstrief Center for Healthcare Engineering HIPAA Compliant Policy Manual.
- Shall track project progress to ensure no access to the data is allowed past project completion.
- Shall notify the Data Manager and Server Manager of project completion, termination of all access to the project data, and removal of all project data from the system.

Data Manager
- Shall be HIPAA certified.
- Shall establish appropriate directories on the HIPAA-compliant server for the project- specific PHI.
- Shall establish and manage access to the project data per the direction of the Project PI.
- Shall import, add, delete, change, update, export, desensitize, store and document the project-specific PHI per the direction of the Project PI.
- Shall act as a RCHE liaison to the Server Manager regarding issues related to RCHE’s HIPAA-compliant servers.
- Upon direction from the Project PI, shall erase or destroy all project-related data and accounts on RCHE’s HIPAA-compliant servers according to Purdue’s Regenstrief Center for Healthcare Engineering Protected Health Information Data Handling and Disposal Policy.
Server Manager

- Shall be HIPAA certified.
- Shall support RCHE’s HIPAA-compliant infrastructure, including server maintenance and storage of project-specific PHI.
- Shall administer the environment, including the updating and configuring of server operating systems, utilities and firewalls to ensure appropriate data protection.
- Shall log server access by users and maintain these records for six years.
- Shall make the logs available when necessary for incident investigation.
- Shall conduct regular backups.
- Shall maintain the ability to recover the data.
- Shall adhere to a policy of minimum necessary access as directed by the Project PI.

Data Access

Only required data shall be accessed by the covered workforce who are participating in a particular project and are authorized to access the data. The data shall be accessed for legitimate business purposes and during the time the project is active.

Data Handling

Researchers interested in using project-specific PHI must be recognized members of an RCHE project. The project PI shall maintain the current list of recognized members. Interested researchers shall contact the Project PI for access to the project data. Only data specific to that project shall be provided to the project researchers. Upon approval, the project PI shall submit the researcher’s name to the Data Manager to allow the researcher access to the appropriate data set. Throughout the project, researchers shall have access to the project data at the sole discretion of the Project PI and must consider all project information, even though possibly de-identified, as confidential. Only those researchers with the “need to know” to properly perform the project shall have access to this information. A workforce member with a “need to know” is defined as someone who requires information because the information is directly related to the duties and activities the person is required to perform as described in their job description.

RCHE employees who are patients of the providers’ offices or hospitals that are subject of a particular study or who have dependents, family members, co-workers or friends who are patients of the providers’ offices or hospitals must follow standard procedures, applicable to all patients, for accessing their own patient information or the information of others. Inappropriate use or disclosure of the data shall be reported to the RCHE HIPAA Liaison.

Research documentation shall be maintained by the Project PI, and the date of research completion shall be tracked. The project completion date shall be periodically reviewed by the Project PI to ensure that access to the data is not provided past the project end date without prior IRB approval. All abstracts, presentations and manuscripts shall be submitted to the Project PI for approval prior to submission for publication. The Project PI may request a recommendation from other key project personnel prior to issuing a decision. Publication approval from the Project PI shall be provided to the researcher within two weeks of submission.
Upon completion of the project, the Project PI shall request from the Data Manager that all system access be terminated and that all project data be appropriately erased or destroyed beyond the ability to recover.

Data Transmission

RCHE researchers shall use Filelocker to transmit data securely. Filelocker is an open source program that has been adopted by Purdue for use by faculty and staff and can securely share data with others both inside Purdue and outside. It is a temporary and secure storage system for sharing files and data. Access to and additional information on the use of Filelocker is available at https://filelocker.purdue.edu. (Purdue career account and password necessary)

Communications

When using or requesting PHI, RCHE shall make reasonable efforts to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose. Appropriate security measures shall be applied for the form of communication being used:

- Be aware of who is around and could be listening. Speak only to intended receiver.
- Use fax cover sheet with “confidentiality” on it.
- Remain at the copier while information is being copied and take all papers when you leave.
- Use Purdue’s Filelocker for sending information or data via email.
- Do not mark mailed documents (campus mail or external carrier) indicating its contents.
- Seal envelope in such a way that tampering would be noticed upon receipt.

RCHE workforce members may not discuss patient information with their friends, family members, spouses, religious leaders, or any other individuals unless allowable by HIPAA. Inappropriate use or disclosure of individually identifiable health information shall be reported to the RCHE HIPAA Liaison or the Director of HIPAA Privacy Compliance. The University may apply sanctions to employees who violate HIPAA policies and procedures.

Security

RCHE shall support the efforts of Purdue to maintain computer and transmission safety, this includes but is not limited to:

- Changing your password often, do not give out your career account or password
- Configuring workstation with password protected screensaver with no more than 15-minute timeout.
- Using recommended antivirus or other security downloads available (http://www.purdue.edu/securepurdue/download/)
- Locking workstation when unattended
- Not transferring files containing PHI to a laptop or mobile device (includes flash drives)
- Not storing PHI on C: drive if network drive is available
- Locking file cabinets where data is stored
- Keeping confidential information in your workspace out of sight
A risk analysis shall be conducted to identify potential security risks and the vulnerability of any area. This shall include the probability of any threats to the integrity of information protected by HIPAA. RCHE security is overseen by the RCHE HIPAA Liaison.

**Retention**

RCHE is required to maintain the required documentation for six years from the date of creation or the date it was last in effect whichever is later. HIPAA retention requirements apply to specific documentation retained by Purdue’s HIPAA Covered Components. The information to be retained includes, but is not limited to:

- Name of researcher
- Contact information for researcher
- Name of study
- Description and purpose of the study
- Type of PHI used
- Timeframe of disclosures

**Disposal**

RCHE employs the following disposal techniques approved by the Information Technology at Purdue (ITaP) security group and HIPAA:

- Documents maintained at RHCE that require disposal shall be shredded or placed in a locked confidential recycling container.
- Employees shall never copy files containing PHI to a laptop or mobile device (phone or flash drive) unless other means are unavailable. Prior approval from the RCHE HIPAA Liaison and Project PI must be obtained if this is necessary.
- PHI shall not be stored on “A” or “C” drives if a network drive is available.
- Data stored on CDs or other removable storage devices shall be erased or destroyed beyond the ability to recover.
- If employee leaves position, computer shall be reimaged after a complete DOD by ITaP to remove all possibility of information recovery.
Breach

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

There are three exceptions to the definition of “breach.” The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate. The second exception applies to the inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

- Notice is to be made to the HIPAA liaison of RCHE of an inadvertent disclosure. The Liaison will notify the Director of HIPAA compliance at Purdue.
- The IT Networks and Security will notify the Director of HIPAA compliance at Purdue should the breach include PHI.
- Business associates of the covered components are required within the Business Associate Agreement, to notify Purdue of any unauthorized use or disclosure by the business associate or its workforce, agents or subcontractors and the remedial action taken or proposed to be taken with respect to the use or disclosure.
- Notification of a potential breach needs to occur immediately upon discovery.

The breach notification should include (as much as possible):

- Description of event
- Description of types of unsecured PHI that were involved – do not list actual data, avoid including sensitive information
- Any steps taken to prevent harm to others
- Any steps the covered entity is taking to investigate breach
- Contact procedures for individuals affected for notification