Procedure #16
Role Based Permissions Guidelines

Purpose

The state designated Regional Health Information Organization, the Rhode Island Quality Institute (RIQI) will implement a range of guidelines and technical safeguards to protect the confidentiality of patient health information in CurrentCare. System access parameters are defined to align with current organizational structures, roles, and information access practices while supporting the need for active security controls and meaningful audit trails within CurrentCare. The purpose of these guidelines is to define how user roles will be controlled.

Scope

These guidelines applies to all Rhode Island Quality Institute ("RIQI") staff members. RIQI "staff members" includes all employees, volunteers, vendors, and subcontractors. These guidelines also applies to all authorized CurrentCare users.

Guidelines Statement

Role-based Permissions (a.k.a., role-based authorization) is a security technique that enables or disables options for accessing functions and/or information in a given electronic system depending on the user's role. A defined set of roles are established for CurrentCare, encompassing a set of rights or permissions to indicate which system functions a user in that role may perform and what information users in that role may work with through a computer terminal. As part of user registration with CurrentCare, the unique identifying information for each authorized user of CurrentCare will be associated with a role. This role will be determined by the participating entity's Delegated User Administrator. When the user signs on to CurrentCare, a user access profile is invoked and the user's permissions related to system functions, patient records and content within those records are controlled accordingly.

Access privileges must be updated to reflect changes in user roles, employment or any other applicable user event. Appropriate security measures will be taken to minimize the possibility of unauthorized access to secure data by those who are no longer authorized to have access to that information.

<u>Responsibility</u>

The entity responsible for assuring guidelines compliance:

- CurrentCare
- RIQI, RIQI's Account Administrator, RIQI's HIPAA Privacy & Security Officer, RIQI's Information Security Officer
- The participating entity and their Delegated User Administrator

User Roles and Permissions

RIQI will maintain *user access permission profiles* to specify which system functions and protected health information (PHI) may be accessed by authorized users according to the specific role classification to which they are assigned. User access permission profiles are based upon two principles:

- First, that access to information must not be so restricted as to interfere with the quality or efficiency of patient care; and
- Second, that access shall be sufficiently restricted to afford privacy and security to patients' information.

Minimum Necessary Rule

Access profiles will comply with the MINIMUM NECESSARY RULE pursuant to a Business Associate Agreement ("BAA") in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and are used to limit electronic access to PHI.

User Awareness of System / Information Access by Role

Participating entities will be responsible for specifying how job descriptions map to defined CurrentCare User Roles. RIQI is responsible for including access levels in training materials to assure that each user is aware of what system functions and information are permitted to be seen and used in their specific role/s. As part of the setup process, the Delegated User Administrator will determine which users for their entity should be assigned which CurrentCare User Role. Users will also be made aware of and trained on access control policies, procedures and system audit practices. The user is responsible for adhering to the intended level of permission granted by user role, organizational affiliation and patient authorization and reporting any discrepancies to the RIQI HIPAA Privacy and Security Officer.

Termination of Access

If a user no longer requires system access, if user permissions change, or if system use audits demonstrate protracted inactivity or unauthorized activity in specific user accounts, modification or termination of access privileges will be processed in CurrentCare as soon as possible and coordinated with the appropriate entities. The participating entity's Delegated User Administrator will notify RIQI immediately if any changes are required for any of their Users. This provision also applies to termination of access to specific types of PHI and/or system functions when the status of any user no longer requires access to specific types of information.

Review of Roles and Permissions Matrix

The user roles and permission matrix used to implement user access permission profiles will be reviewed and revised periodically, upon request of a participating organization when a new role is created, when a role changes significantly, or when experience shows a need to make a modification.

Compliance

Any violation of these guidelines by any RIQI employee will subject the employee to disciplinary action or immediate discharge. Any RIQI employee having knowledge of any violation of these guidelines shall promptly report such violation to Human Resources.

Any violation of these guidelines by any member of a participating entity's organization shall be promptly reported to the RIQI HIPAA Privacy and Security Officer. If a participating entity is found to be in violation of these guidelines, legal action may be taken - including the potential termination of the entity's rights to use CurrentCare.

Version	Effective Date	Statement of Change
01	March 27, 2008	Original document
02	July 22, 2013	Removed Risks & Controls, user table, and procedure elements.
03	See signature date below	Changed from Policy to Guidelines

Ver 3. _____

Director/Manager Date