Policy #1
CurrentCare End-User Registration Policy

Purpose

It is important that all CurrentCare users be known by their physical identity to the organization and with which they are affiliated and known by an online identity to the CurrentCare system. The purpose of this policy is to establish the requirements to register provider organizations and their affiliated personnel as users of CurrentCare.

Scope

This policy applies to all departments and positions at all levels, including full-time, part-time, and temporary positions. This policy also applies to all CurrentCare users.

Policy Statement

All users of the CurrentCare system will gain access to the system as a result of their affiliation with an end-user organization that has met specific qualifications and are registered in the system. Organizations that qualify to become registered CurrentCare user sites will be required to meet specific technical, legal and management requirements. As an essential step in assuring the confidentiality and accurate auditability of health information in CurrentCare, the user site registration process establishes relationships between registered organizations and their affiliated users and describes how these relationships will be maintained in the system.

To register in CurrentCare, each prospective user site must agree to and abide by the terms of a standard Data Use Agreement that addresses specific technical, confidentiality, data use and management requirements. User sites must also complete a Participation Readiness Attestation Form outlining the prerequisites for a smooth CurrentCare implementation.

Registered user sites must designate a Delegated User Administrator to serve in the following capacity: (a) verify the physical identity of users affiliated with the organization (as per the User Authentication Policy); (b) routinely update user information required to maintain current identifying information; and (c) notify the RIQI Operations Program Support of any significant user and/or technical issues.

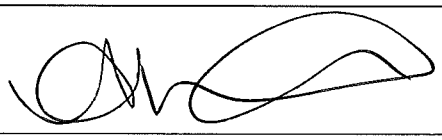
The RIQI Operations Program Support staff will be responsible for creating and deactivating new users.

Registered user sites must agree to support user training and education necessary for responsible and correct use of the system and observation of essential policies and procedures.

Compliance

Any violation of this policy will subject the employee to disciplinary action, up to and including discharge. Any RIQI employee having knowledge of any violation by an employee of the policy shall promptly report such violation to Human Resources. Any RIQI employee having knowledge of any violation by an end-user shall promptly notify the security officer.

Version	Effective Date	Statement of Change
01	January 22, 2009	Original document
02	November 29, 2012	Format change; Added revision control
03	March 20, 2014	Removed procedure; Minor modifications to policy language; Removed "Responsibility" section
04	See signature date below	Per Audit & Compliance/Policy & Legal Committee: Minor grammatical changes to Policy Statement section; Language added to the Compliance section regarding notification of the Security Officer

Ver 4.  7/29/14

Alok Gupta, COO & CIO Date