Policy #12
Response to Security Incident Policy

Purpose

The Response to Security Incident Policy describes the process by which RIQI will investigate, confirm and respond to a confirmed breach of the security and/or confidentiality of protected health information (PHI).

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 vendors, contractors and authorized CurrentCare users.

Policy Statement

The state designated Regional Health Information Organization, the Rhode Island Quality Institute (RIQI), its contractors, and the authorized users of CurrentCare will strive to prevent any breach of Current Care, electronically or otherwise, and implement privacy and security measures to protect the confidentiality of information in CurrentCare. A breach of security means any unauthorized access to the CurrentCare system and/or of its security safeguards of which RIQI becomes aware, and a breach of confidentiality means the use or disclosure of confidential information by an individual(s) for purposes other than those for which the person is authorized.

RIQI will implement and maintain security measures to protect the protected health information of enrollees in CurrentCare from unauthorized use or disclosure, and will respond to any confirmed breach of security and/or confidentiality according to this policy, and will comply with applicable state and federal laws.

RIQI, its Response Team, Security Office, Privacy Officer and/or RIQI's agents the CurrentCare system vendor, and the authorized provider user sites will monitor CurrentCare and respond to any suspected or confirmed breach.

1. RIQI will abide by all applicable federal, state and local laws, rules and regulations pertaining to the security of PHI.

    a) PHI is any information that, individually or in combination, could identify the person should someone see or overhear it. Certain information is unique to an individual and by itself can identify that person. If health information is linked with the following unique items, it qualifies as PHI:

    - Name, social security number, street address, driver's license number

- Telephone or fax numbers, e-mail address or website addresses/URL
- Medical record or patient identification numbers, including account number, health plan ID numbers
- Biometric identifiers, including finger and voiceprints
- Full-face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

b) A security breach is an internal or external act that bypasses or contravenes security policies, practices or procedures.

2. RIQI, its contractors, and authorized users of CurrentCare have the obligation to report any suspected breaches of security and/or confidentiality of CurrentCare. RIQI policies, Data Sharing Partner Agreements and Data Use Agreements include a requirement and method for reporting Breaches of Unsecured Protected Health Information. If an allegation of a breach of security and/or confidentiality is made by a patient or others to any staff member at a provider organization that is an authenticated user, those allegations shall be made using the formal complaint form submitted by the CurrentCare provider organization to RIQI. (See CurrentCare Complaints Policy).

3. RIQI will respond to any confirmed breach of confidentiality, described as:

   a) Unintended disclosure – accidental disclosure of PHI to unauthorized users of CurrentCare or other persons

   b) Intentional and unauthorized disclosure – willfully disclosing PHI to unauthorized person(s).

   c) Loss of control over CurrentCare due to system failure or other physical loss – e.g., theft or system malfunction that results in loss of control over security and confidentiality of PHI.

4. The RIQI Response Team, Security Officer and/or Privacy Officer will evaluate any suspected breach in order to determine if an investigation is warranted.

   a) The RIQI Response Team, Security Officer and/or Privacy Officer may decide that an alleged breach does not require investigation if:

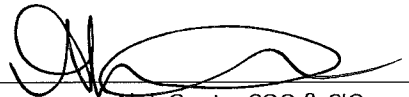
      - The length of time that has elapsed since the date of the complaint makes an investigation no longer practicable or desirable;

- The subject matter of the complaint is not made in good faith or there is enough evidence to confirm that the complaint is not legitimate.

Compliance

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

Version	Effective Date	Statement of Change
01	July 1, 2008	Original document
02	November 29, 2012	Format change; Added revision control
03	March 20, 2014	Removed Procedure section; Minor language revisions
04	See signature date below	Changes made after Audit & Compliance/Policy & Legal Committee Review: Changed Policy Name to "Response to Security Incident Policy"; Minor changes to language in Policy Statement section

Ver 4.  7/29/14

Alok Gupta, COO & CIO Date