



<b>currentcare</b> <b>POLICY AND PROCEDURE</b>	
<b>Subject:</b> Response to Breach of currentcare	<b>Related Policies:</b> Complaints Policy, Confidentiality Policy, Notification of Breach
<b>Stakeholder Group:</b> Steering Committee	<b>Submission Date:</b> July 24, 2008
<b>Target Implementation Date:</b> July 2008	<b>Date of Scheduled Review:</b>

**BRIEF DEFINITION:** The Regional Health Information Organization (RHIO), its contractors, and the authorized users of currentcare will strive to prevent any breach of currentcare – either electronically or otherwise – and implement privacy and security measures to protect the confidentiality of information in currentcare. *The Response to Breach of currentcare Policy* describes the process by which the RHIO will investigate, confirm and respond to a breach of security and/or confidentiality of protected health information (PHI). A breach of security means any unauthorized access to the currentcare system and/or of its security safeguards of which the RHIO 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.”

**BACKGROUND AND PURPOSE:** The RHIO will implement and maintain security measures to protect the personal health information of enrollees in currentcare from unauthorized use or disclosure, and will respond to any breach of security and/or confidentiality according to this policy, and will comply with applicable state and federal laws. This policy informs the community of the actions that the RHIO will take in response to any breach.

---

**RESPONSIBILITY:** The RHIO, its Response Team and Privacy Officer, the currentcare system vendor, and the authorized provider user sites will monitor currentcare and respond to any suspected breach. The RHIO will make this policy known through educational materials and online resources.

**POLICY:**

- 1. The RHIO will abide by all applicable federal, state and local laws, rules and regulations pertaining to the security of PHI and for any security incident related to currentcare.**
  - 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 web site 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. The RHIO, its contractors, and authorized users of currentcare have the obligation to report any *suspected* breaches of security and/or confidentiality of currentcare.** The RHIO Employee policy and the currentcare User Agreement will include a requirement and method for reporting suspected breaches. 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 user organization to the RHIO (see Complaint Policy).
- 3. The RHIO will respond to any confirmed breach of confidentiality, described as:**
- a. **Unintended disclosure** - accidental disclosure of PHI to unauthorized users of the HIE 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 RHIO Response Team/Privacy Officer will evaluate any suspected breach reported via a formal complaint in order to determine if an investigation is warranted.**
- a. The RHIO Response Team/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.

## Procedure

### I. Investigation of suspected breach of security or confidentiality

**A. The RHIO Response Team/Privacy Officer shall investigate a suspected breach of security and/or confidentiality that has been evaluated and determined to present a current risk and has been reported in good faith.**

1. If the decision is made to proceed with an investigation, it is the responsibility of the RHIO Response Team/Privacy Officer to investigate the allegation and consult appropriate resources to make the following determinations:
  - The type of breach (none, security only, or security and confidentiality)
  - The scope of the breach, if it occurred (i.e., the number and identities of individuals whose PHI may have been breached, the severity of the security breach, etc.)
  - If possible, the individual(s) that caused or contributed to the breach.

### II. Confirmed breaches of security only

**A. The RHIO Response Team/Privacy Officer shall work with the currentcare system vendor to determine the appropriate Mitigation Plan, depending upon the type and scope of the security breach.** The intention of a Mitigation Plan is to reduce any chance that a similar breach of security occurs. The Mitigation Plan should identify the response to the breach including:

1. Action limited because breach was low-severity, one-time, or immediately corrected. Reporting the breach to Data Sharing Partners, currentcare system vendor, and any required parties is necessary only; and
2. Identification of the cause of contributing factor(s) of the security breach and identifies the corrective action.
3. An assessment of whether or not the breach was intentional or accidental and the corresponding action items as a result of the assessment.

### III. Confirmed breaches of security and confidentiality

**A. When the RHIO Response Team/Privacy Officer confirms that a breach of security and confidentiality has occurred and resulted in the unauthorized disclosure of PHI, the RHIO Response Team/Privacy Officer will take the following steps:**

1. Notify the individual(s) and if applicable, the individual(s) employer found to have violated the confidentiality policy (either at the RHIO, at a currentcare organization, or other) of the Violations of Breach policy, and, where appropriate, notify them of the process by which a written appeal request may be submitted.
2. Report any breaches to the Data Sharing Partners and the currentcare system vendor.
3. If the site(s) of the breach of confidentiality is the RHIO or entities that have signed agreements with the RHIO, then the RHIO Response Team/Privacy Officer will work with those site(s) to develop the appropriate Mitigation Plan, which includes:

- Identifying the cause of the breach of confidentiality and take appropriate action (see Violations of Breach policy).
- Review and correct where appropriate any policy or procedure that directly caused or contributed to the breach of confidentiality.

#### **IV. Notification**

**If applicable, the RHIO may provide notice to the individuals whose PHI has been breached if unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person and the breach poses a significant risk of identity theft or other harm in accordance with the Notification of Breach Policy.**