


 Approved

currentcare POLICY AND PROCEDURE	
Subject: Notification of Breach	Related Policies: Patient Authorization, Enrollment, Uniform Patient Authorization Form, Complaints, Response to Breach
Stakeholder Group: Steering Committee	Submission Date: July 24, 2008
Target Implementation Date: July 2008	Date of Scheduled Review: TBD

BRIEF DEFINITION: The Regional Health Information Organization (RHIO), its contractors, and the authorized users of currentcare will strive to prevent breaches – electronically or otherwise – and maintain privacy and security measures to protect the confidentiality of information in currentcare. The notification of breach policy describes the process by which the RHIO will notify individuals regarding a confirmed breach of security of currentcare when unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or a person without authority to acquire said information, including when the breach poses a significant risk of identify theft or causes other harm.

BACKGROUND AND PURPOSE: The RHIO will notify individuals when unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or a person without authority, including when a confirmed breach in the security of the system poses a significant risk of identity theft or other harm.

Responsibility:

The RHIO, its Response Team and Privacy Officer.

POLICY

- I. **Confirmed breaches of security or confidentiality of currentcare will invoke certain actions to determine the degree of risk and impact of the breach and, under specific circumstances, provide notification of the breach to effected individuals.**

PROCEDURE

- A. In cases where, pursuant to the Response to Breach Policy, the RHIO Response Team/Privacy Officer confirms that a breach of security or confidentiality has occurred and resulted in the unauthorized disclosure of protected health information “PHI”, the RHIO Response Team/Privacy Officer will take the following steps:

1. Determine whether or not the information breached was encrypted or unencrypted.
 2. Determine the reasonable likelihood that such unencrypted information was accessed by an unauthorized person.
 3. Determine whether or not the information breached includes personal information, including an individual's first name or first initial and last name in combination with other personal data elements, such as, address and date of birth, when either the name or the other data elements are unencrypted and includes PHI of the individual.
 4. Determine whether or not the breach of the security of the data poses a significant risk of identity theft or other harm.
- B. If it is determined that the information breached was encrypted and there is not a reasonable likelihood that the encrypted information was rendered viewable, no further action is necessary.
- C. If the RHIO Response Team and/or Privacy Officer determine that the breach does not pose a significant risk of identity theft or other harm, no further action is necessary.
- D. If the RHIO Response Team and Privacy Officer determine that the breach of the security of the system poses a significant risk of identity theft or other harm, the RHIO Response Team and/or Security Officer shall in the most expedient time possible, notify the individual(s) whose information was disclosed as a result of a breach.
- E. The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the notification will only be made after law enforcement determines it will not compromise the investigation.
- F. Notification of breach to effected individuals will be made by one of the following methods:
1. Written notice; or
 2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code and assuming no PHI is included in the notice; or
 3. Substitute notice, if the RHIO demonstrates that the cost of providing notice would exceed twenty-five thousand dollars (\$25,000), or that the affected class of subject persons to be notified exceeds fifty thousand (50,000), or the RHIO does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - a. E-mail notice when an email address is supplied; or
 - b. Conspicuous posting of the notice on the RHIO's website; or

- c. News media alert.
4. Notification of breach shall include the following information, if known:
- a. The circumstances of the breach and how many people were affected.
 - b. The steps that have been taken and will be taken by the RHIO Response Team/Privacy Officer to respond to the breach.
 - c. The steps that consumers may choose to take next, if applicable.
 - d. Contact information for the RHIO if the consumer has any additional questions or concerns.