

Policy #71
Notification of Breach of Unsecured Protected Health Information Policy

Purpose

Rhode Island Quality Institute (“RIQI”) and its contractors and vendors will strive to prevent breaches of Unsecured Protected Health Information (“PHI”) and personal information (“PI”) electronically or otherwise, and maintain privacy and security measures to protect the confidentiality of PHI and PI.

Pursuant to the Health Insurance Portability and Accountability Act (“HIPAA”) and Regulations promulgated there under, RIQI will notify covered entities when Unsecured PHI has been acquired, accessed, used or disclosed by an unauthorized person, when a confirmed breach of the security of the system does not fall within a statutory exception or unless there is a low probability that the PHI has been compromised.

Scope

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

Policy Statement

Confirmed breaches of the security or privacy of Unsecured PHI will invoke certain actions to determine the probability that the PHI has been compromised based on a risk assessment and, under specific circumstances, notification of the breach will be made to the covered entity or the affected individual as required by law.

Procedure

- A. RIQI has implemented reasonable and appropriate Administrative, Physical and Technical Safeguards to protect the confidentiality, integrity and availability of PHI and PI in its possession.
- B. RIQI has implemented reasonable systems for the discovery and reporting of a breach of PHI or PI. A “breach” of PHI is the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI.
- C. When a breach has been reported, an investigation into the breach will be conducted.
- D. The investigation and steps taken will be thoroughly documented. If the conclusion of the investigation is that no breach occurred, no further action is necessary, but the investigation and conclusion will be thoroughly documented.

- E. If it is confirmed that a breach of security or confidentiality has occurred and has resulted in the unauthorized disclosure of PHI, the following risk assessment steps will be taken:
 - 1. Determine whether or not the information breached was Unsecured. Unsecured PHI includes information not secured through encryption or destruction, and is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of HHS in guidance issued under Section 13402(h)(c) of Public Law 111-5.
 - 2. Determine the reasonable likelihood that such information was accessed by an unauthorized person.
 - 3. Determine the probability that the PHI has been compromised based on a risk assessment of at least the following factors: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated.
- F. The risk assessment will be documented thoroughly, including the actions taken, the conclusions of the assessment and the basis for the determination that there was or was not a low probability that the PHI was compromised.
- G. If it is determined that the information breached was secured and there is no reasonable likelihood that the secured information was rendered usable, readable or viewable by an unauthorized person, no further action is necessary, but the determination and conclusion will be documented.
- H. If it is determined that the information breached was Unsecured, but the circumstance of the breach falls within one of the exceptions to HIPAA (45 C.F.R. § 164.42), so notification is not required, such determination will be documented.
- I. If it is determined that the breach of the security of the system demonstrates that there is more than a low probability that the PHI was compromised, RIQI will as soon as possible, but no later than 60 days after the discovery of the breach, notify the covered entity whose patients' information was disclosed as a result of the breach, and the determination and conclusion will be documented.
- J. If it is determined that the information breached was Unsecured and notification is required, an analysis of the requirements for notification of the State in which the individuals reside will be conducted and documented.
- K. If notification to law enforcement or another regulatory body or agency is required under State law, such notification, at the request of covered entity, will be made to the regulatory body or agency in accordance with State law.
- L. If State law requires notification to the individual, notification will be made in accordance with State law, if required by the covered entity.
- M. Notification to the individual may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the


notification will be made after law enforcement determines it will not compromise its investigation.

- N. Notification of a breach to the covered entity will be in plain language and include at a minimum:
1. a brief description of what happened, including the date of the breach and discovery of the breach;
 2. a description of the type of Unsecured PHI or other personal information that was involved in the breach;
 3. any steps individuals should take to protect themselves from potential harm resulting from the breach;
 4. a description of the investigation into the breach, mitigation of harm to individuals, and protection against further breaches; and
 5. contact procedures, which will include a toll-free telephone number, an e-mail address, website or postal address.
- O. The notification must include any additional information required by applicable State law.
- P. If the breach involves more than 500 residents of a state or jurisdiction, RIQI will provide notice of such fact to covered entity.
- Q. A log of any and all breaches of Unsecured PHI of less than 500 individuals will be maintained and reported to covered entity.
- R. Business Associates and vendors, through their contracts and/or Business Associates Agreements with RIQI will be required to provide notification of a breach to RIQI so affected individuals or covered entities can be notified, as necessary. Business Associates must provide all available information without delay.
- S. Documentation will be maintained of each individual or covered entity notified, each notification provided to HHS and any other notification to the Secretary of HHS as required by law.

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	August 17, 2011	Original document
02	December 13, 2013	Minor language revisions; Removed Risks & Controls sections
03	See signature date below	Per Audit & Compliance/Policy & Legal Committee Review: Merged procedure with the policy and modified the following language in the Policy Statement: "notification of the breach will be made to the covered entity or the affected individual as required by law."

Ver 3.  7/29/14
 Alok Gupta, CIO & COO Date