LOUISIANA
HEALTH CARE
QUALITY FORUM

WORKING TOGETHER FOR A HEALTHIER STATE

Security Breach Response Protocol

Procedures for Responding to a Security Breach Involving Electronic Protected Health Information

TABLE OF CONTENTS

Page

Definitions

Security Incident Reporting (Low-Medium Risk)

Security Breach Response Team

Response to a Security Breach

Post-Incident Actions

Appendix

INTRODUCTION

The purpose of this Security Breach Response Protocol ("Protocol") is to establish formal documented procedures to be followed when LHCQF becomes aware of instances of unauthorized access to or disclosure of, patients' protected health information ("PHI"), in accordance with applicable state and federal laws and LHCQF's policies.

This Protocol describes a recommended process for responding to such incidents, the conditions whereby this process is invoked, the resources required, and the course of recommended action. The primary emphasis of activities described within this Protocol is the return to a normalized (secure) state as quickly as possible, while minimizing the impact to LHCQF, LHCQF's customers and to the individuals/patients. However the appropriate type of response will depend on the specific facts of each PHI disclosure incident and applicable federal and state laws, and thus the process recommended by this Protocol may have to be revised accordingly.

This Protocol establishes the Security Breach Response Team, which shall have the responsibility for the actions contained herein.

DEFINITIONS

1. **Protected Health Information (PHI):** as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), protected health information[1] is defined as health information, including demographic information collected from an individual, and:
   (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
   (2) Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
      (i) that identifies the individual; or
      (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

2. **Security Incident:** a Security Incident[2], as defined by HIPAA, means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. A Security Incident poses a threat to LHCQF's or LHCQF's customers' physical environment or information systems. Each Security Incident will be evaluated and assessed a risk score based on the threat, vulnerability and impact of the Incident (See Appendix).

   Examples of a Security Incident assessed as Low (score of 4 or less) may include, but are not limited to:
      a. Pings on a firewall;
      b. Malware;
      c. Denial-of-service attacks that do not result in a server taken off-line;

[1] 45 C.F.R. 160.103
[2] 45 C.F.R. 164.304

d. Port scans;
e. Attempts to log on to a system or application, or enter a database with an invalid password or user name.

Examples of a Security Incident assessed as Medium (score of 5-6) may include, but are not limited to:

a. PHI sent to an unintended recipient;
b. An employee using another user's identification;
c. Unauthorized access to PHI by an employee;
d. Failure to comply with LHCQF's privacy and security policies and procedures.

3. **Security Breach:** A Security Incident assessed as High (score of 7-8) or Severe (score of 9), will be considered a Security Breach, requiring activation of this Protocol.

   Examples of a Security Breach may include, but are not limited to:

   a. Intentional, unauthorized access to LHCQF's customers' data with the intent to sell, transfer, use for commercial advantage, personal gain, or malicious harm;
   b. Theft or loss of portable media (such as unencrypted laptops or USB sticks) containing electronic PHI;
   c. Law enforcement investigations that involve LHCQF's information or personnel that may impact LHCQF's or LHCQF's customers' information, systems, facilities or workforce;
   d. A Security Incident that, although unintentional, has a substantial risk of harm to a high number of individuals.

PROCESS

1. Security Incident Reporting (LOW-MEDIUM RISK):

   a. Security Incident (Low Risk): Unsuccessful Security Incidents, such as attempts to access, misuse, disclose, modify or destroy information or physical assets shall be logged and tracked by LHCQF in accordance with LHCQF's policies and procedures. The Health IT Director or his/her designee shall be responsible for reviewing such logs and taking appropriate actions.

   b. Security Incident (Low – Medium Risk): Any employee, data owner or customer who believes that a successful Security Incident has occurred, shall immediately notify the Health IT Director upon becoming aware of such Security Incident.

2. The Executive Director or his/her designee will conduct an investigation, coordinate the investigation with stakeholders, as appropriate to the incident, including, but not limited to: Information Security, customers and business associates, Human Resources, and others, as appropriate. The Executive Director or his/her designee shall maintain written documentation of the Security Incident, such as a description of the incident, root cause of the incident, remediation actions taken, and corrective measures applied.

   If, during the investigation, the Executive Director determines that a Security Breach has occurred, he/she will immediately activate the Security Breach Response Team.

3. Security Breach Response Team:

    a. Security Breach Response Team ("Team") Composition **–** The Executive Director, or his/her designee, will be responsible for activating the Security Breach Response Team. Depending on the circumstances of the Security Breach, the Team will be comprised of appropriate representatives from the organization and/or customer affected.

    b. Team Objectives **–** The Team will take all commercially reasonable steps to minimize the potential negative impact of the Security Breach and restore services to a normalized and secure state of operations as soon as possible. In addition, the Team will:

        i. Coordinate and oversee the response to a Security Breach in accordance with the requirements of state and federal laws and LHCQF's policies;
        ii. Where appropriate or as required by law, inform the affected individuals and third parties of action that is recommended or required on their behalf;
        iii. Provide clear and timely communication to all interested parties.
        iv. Conduct a post-Security Breach review;
        v. Ensure appropriate actions are taken to prevent a recurrence;
        vi. Establish, maintain and document periodic Security Breach Response Protocol testing;
        vii. Review the Security Breach Response procedures at least annually and update as necessary.

4. Response to a Security Breach

    a. Activation of the Team - The Executive Director or his/her designee shall be responsible for activating the Team and providing an initial report to the Team and Executive Management.

       Note: The following procedures may repeat or be concurrent depending upon the incident.

    b. Determination of the Risk - The Team will assess the risk to LHCQF or LHCQF's customer posed by the Security Breach by developing a risk assessment scoring tool (See Appendix) that is based on:

        - Threat (probability)
            - Malicious – intentional, targeted at LHCQF
            - Inadvertent – untargeted threat

        - Impact (criticality)
            - Determine the potential damage and business impact of the incident
            - Determine if the incident has or will affect businesses or resources outside of the LHCQF network

        - Vulnerability (exposure)

- Determine if the incident is localized in nature or company wide

c. Communications and Notifications - The Executive Director will coordinate all internal and external communications and notifications as appropriate to the circumstances, including, but not limited to:

- State and/or federal law enforcement
- Regulators
- Media
- Customers, vendors and clients
- Employees

In addition:

- Only the designated spokesperson, i.e., the Executive Director, or his/her designee, shall speak directly with the media;
- All notifications will be documented, including date and time of notification, who was notified and who made the notification;
- All communications pertaining to a Security Breach must be on a confidential, need-to-know basis;
- The Executive Director shall monitor and communicate ongoing progress of the Security Breach investigation.

d. Recording the Incident – The Executive Director or his/her designee shall securely maintain all documentation relating to the Security Breach, including, but not limited to: a log of all activities and events in response to the Security Breach.

e. Ongoing Security Response Activities – during the course of the investigation, the Executive Director, or his/her designee, working with the Team may:

i. Determine what additional parties need to be involved in the issue resolution;
ii. Transfer some or all responsibility to the LHCQF Security Breach Response Team (SBRT) upon completion of the risk assessment. The IRT is under the direction of the Executive Director or his/her designee;
iii. Identify and contact additional functional areas and/or individuals, as needed to respond.

5. Post-incident actions - The following actions will be initiated by the Executive Director and require involvement of the Team members or individuals, as appropriate:

a. Meet with the Team and other appropriate individuals to assess the actual impact of the Security Breach;
b. Lead efforts to determine root cause, if not already discovered;
c. Designate responsibility for any follow-up security remediation activities to the appropriate business area/service line;
d. Ensure that appropriate Security Breach notification is conducted to covered entities where LHCQF is the business associate;
e. Ensure each functional area has maintained chain of custody for collected evidence;

f. Identify and recommend the appropriate retroactive and prospective corrective actions to the Executive Committee;
g. Communicate final reporting to Executive Management, and others, as appropriate;
h. Declare the Security Breach response as completed;
i. Conduct “Lessons Learned” session(s);
j. Review/revise the Team procedures if needed;
k. Provide final report to Executive Management, the Executive Committee, and the Board of Directors.

APPENDIX

SECURITY RISK ASSESSMENT PROCESS

The Team will assess risk based on: (a) protecting the safety and personal well-being of the LHCQF workforce and others; and (b) protecting the confidentiality, integrity, and availability of the LHCQF information and information assets.

Risk will be assessed using the following three factors:

1. Threat – the likelihood (or actual event) that puts personnel or information resources at risk of harm, loss of confidentiality, integrity, or availability, or corruption of data;
2. Vulnerability – the exposure of personnel or information to potential threats;
3. Impact – the impact of the loss of information or personnel. This can be quantified in financial terms or qualified by importance to business operations (i.e., high, medium, or low.)

	Threat	Vulnerability	Impact
High	• An actual security breach has occurred or the probability of occurrence is extremely high (over 70%) • The nature of the threat is malicious in nature and cannot be effectively managed with existing controls • The threat is demonstrable and pervasive in the physical or computing environments	• Exposure to a particular threat is extremely high • Large volume of un-patched systems • Exposures that are easily gained • Large amount of data available in a particular facility	• Situation where personnel are at serious risk of harm • Financial impact of loss of data or system assets is significant • Security incident may cause significant embarrassment to LHCQF, LHCQF's customers, or individuals through media attention • Mitigation of vulnerability would be a serious impact to business operations • Significant operational impact resulting in the impact of critical business recovery time objectives • Estimated impact: over $500,000

Medium	• The probability of an actual security breach occurring is likely (30-70%) • The threat can be managed somewhat effectively with existing controls • The threat has been demonstrated to be effective against vulnerable systems – low number of incidents reported	• Exposure to a particular threat is moderate in scope • Measurable amount of information systems that are exposed • Access to systems, data, or personnel is moderately difficult to gain	• Financial impact of loss of data or system assets is measurable but not significant • Risk is not posed to PHI or other information assets of a confidential nature • Mitigation of vulnerability is not a significant impact to business operations • An incident that results in or is likely to result in significant impact to operations, including exceeding critical business unit maximum allowable delays • Estimated impact: Between $50,000-$500,000
Low	• The probability of an actual security breach occurring is low (less than 30%) • The threat can be managed effectively with existing controls • The threat is conceptual or perceived – no known incidents reported	• Exposure to a particular threat is low • Negligible amount of information systems that are exposed • Access to systems, data, or personnel is difficult to gain	• Financial impact of loss of data or system assets is not significant • Risk is not posed to sensitive information assets • Mitigation of vulnerability does not impact business operations • Minor data communications interruption • Estimated impact: Under $50,000

The Team must evaluate the security event using the above criteria as a guideline to determine the appropriate risk for each factor. A high-level risk posed against a low-level criticality may be determined to be of low-medium overall risk to LHCQF.

The following procedure for evaluating the security event shall be used to determine if the event should be classified as a Security Incident or a Security Breach, and to drive the appropriate levels of response.

For each category (Threat, Vulnerability, Impact), the risk-level is scored as follows:

- **High** = 3 points
- **Medium** = 2 points
- **Low** – 1 point

EXAMPLE

	Threat	Vulnerability	Criticality	TOTAL
High	3			3
Medium		2	2	4
Low				0
TOTAL	3	2	2	7

Once each area is scored, total the values across the table, then down, to gain the Overall Risk Rating.

Each area will be assigned a score and the total will allow for ranking the risk:

- **SEVERE (or Critical if non-system related): 9 points**
- **HIGH: 7 - 8 points**
- **MEDIUM: 5 - 6 points**
- **LOW: 3 - 4 points**