Data Breach Response Policy

Last Update: *February 2022*

1. Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

GP HERO Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how GP HERO's established culture of openness, trust and integrity should respond to such activity. GP HERO Information Security is committed to protecting GP HERO's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

2. Background

This policy mandates that any individual who suspects that a theft, breach or exposure of GP HERO Protected data or GP HERO Sensitive data has occurred must immediately provide a description of what occurred via e-mail to Helpdesk@GP HERO.org, by calling 555-1212, or through the use of the help desk reporting web page at http://GP HERO. This e-mail address, phone number, and web page are monitored by the GP HERO's Information Security Administrator. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

3. Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of GP HERO members. Any agreements with vendors will contain language similar that protects the fund.

4. Policy Confirmed theft, data breach or exposure of GP HERO Protected data or GP HERO Sensitive data

As soon as a theft, data breach or exposure containing GP HERO Protected data or GP HERO Sensitive data is identified, the process of removing all access to that resource will begin.

The Executive Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Infrastructure
- IT Applications
- Finance (if applicable)
- Legal
- Communications
- Member Services (if Member data is affected)
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Executive Director

Confirmed theft, breach or exposure of GP HERO data

The Executive Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

As provided by GP HERO cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a communication plan.
Work with GP HERO communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

Ownership and Responsibilities
Roles & Responsibilities:

- Sponsors - Sponsors are those members of the GP HERO community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any GP HERO Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Information Security Administrator is that member of the GP HERO community, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the GP HERO community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

5. Enforcement

Any GP HERO personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

6. Related Standards, Policies and Processes

None.

7. Definitions and Terms

None.

8. Revision History

Date of Change	Responsible	Summary of Change
February 2022	GP Hero Policy Team	New Policy