CITY OF HARTFORD

DEPARTMENT OF HEALTH AND HUMAN SERVICES
131 Coventry Street
Hartford, Connecticut 06112
Ph: (860) 757-4705
Fax: (860) 722-6720
www.hartford.gov

LUKE A. BRONIN
Mayor

LIANY ARROYO
Health Director

CAREWare Data Breach Response Policy

1.0 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. The policy will be made easily available to all CAREWare End Users via email and will posted on the www.ryanwhitehartford.net website.

City of Hartford Metro Hartford Innovation Service's (MHIS) intentions for publishing a Data Breach Response Policy for the CAREWare data system are to focus significant attention on data security and data security breaches and how City of Hartford's established culture of openness, trust and integrity should respond to such activity. City of Hartford Metro Hartford Innovation Service is committed to protecting City of Hartford's employees, citizens, community partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.1 Background

This policy mandates that any individual who suspects that a breach or exposure of City of Hartford's Protected data or City of Hartford's Sensitive data via the CAREWare system or through any other agency web-based platforms, has occurred must immediately provide a description of what occurred via e-mail to the Ryan White Part A Hartford Recipient office Senior Project Manager Angelique Croasdale-Mills at croaa001@hartford.gov or by calling 860-757-4706. This response must be provided within 3 (three) days of the breach. The Ryan White Part A Hartford office Systems Analyst Peta-Gaye Nembhard should be courtesy copied in all written communication to nembp001@hartford.gov . This team will investigate all reported data breaches and exposures to confirm if a breach or exposure has occurred on the City's server. If a breach or exposure has occurred, the City of Hartford's Information Security Administrator will follow the appropriate procedure in place. All agencies will be required to provide a written action report to the City of Hartford. This action report should include technical data valuable to assisting MHIS in mitigating the risk and source of breach.

2.0 Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, or otherwise handle personally identifiable information or Protected Health Information

(PHI) in the CAREWare database that is securely housed and maintained by the City of Hartford. Any agreements with vendors will contain similar language.

3.0 Ownership and Responsibilities

Roles & Responsibilities:

- Database Administrator(s) ("DB") are those members of the City of Hartford organization that have primary responsibility for maintaining the CAREWare server(s). DB Administrators may be designated by City of Hartford's Ryan White Senior Project Manager and Director of Metro Hartford Innovation Systems 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 City of Hartford Metro Hartford Innovation System team, designated by the Director of Innovation System, who provides administrative support for the implementation, oversight and coordination of security procedures
- Users include all End Users with authorized permissions to access the web-based CAREWare platform to enter Ryan White Program. It is the responsibility for all end users to only add applicable data into the database, and not knowingly or intentionally input data that is erroneous or may causes errors within the database

4.0 Definition of Breach

A "breach" is hereby defined as a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve financial information such as credit card or bank details, personal health information (PHI), Personally identifiable information (PII), trade secrets of corporations or intellectual property. Most data breaches involve overexposed and vulnerable unstructured data – files, documents, and sensitive information

5.0 Policy Confirmed data breach or exposure of City of Hartford Protected data or City of Hartford Sensitive data

As soon as a data breach or exposure containing City of Hartford Protected data or City of Hartford Sensitive data is identified, the process of removing all access to the CAREWARE server will begin.

The Director of Metro Hartford Innovation Services will lead an incident response team to handle the breach or exposure to determine whose data may have been breached or exposed.
In the event of a breach, all involved parties should make a best effort to save and digitally verify their logs for future examination. These logs should be shared with MHIS and any parties involved in investigating and remediating the breach.

There is no expectation of privacy for actions taken on the database. All actions can and will be logged. Date entered in the CAREWare platform are sensitive and protected under HIPAA, and therefore are monitored and controlled by database administrators.

6.0 Enforcement

Any Ryan White Organization found in violation of this policy may be subject to access termination of their network connection and any legal fees (excluding State Entities) associated with said breach. For State entities, any recourse shall go through the Connecticut Claims Commission as provided under Chapter 53 of the Statutes of the State of Connecticut.