Hartford Data Collaborative: Data Security Plan & Policy

The Connecticut Data Collaborative (CTData)'s Hartford Data Collaborative (HDC) adheres to data security and privacy standards under state and federal laws and regulations. This data security plan includes HDC's legal and governance structure for managing data, its data management processes, and its data access and security processes.

A. Governance & Legal Structure

The key HDC legal and governance documents—the Enterprise Memorandum of Understanding (EMOU), the Data Sharing Agreement (DSA), and the Data Use License govern HDC's data sharing and integration:

- *Enterprise Memorandum of Understanding* (EMOU) outlines HDC's purpose, mission, the process for signing onto the EMOU, and the HDC request and approval process.
- *Data Sharing Agreement* (DSA) describes the terms and conditions for transferring, storing, and managing data
- *Data Use License* (DUL) outlines the responsibilities of data recipients or users of integrated data and is required to be signed by data requesters prior to the release of integrated data.

The key legal documents are available from HDC staff upon request.

HDC's governing bodies and staff carefully review and consider data requests, including which parties will have access to the data and how the data will be used. Parties interested in obtaining integrated data from HDC members must complete a *Data Application Request* (Data License Request) that lists the specific data fields requested, the justification for the data, how the data will be transmitted, and all the parties that will have access to the data. The HDC Data Oversight Committee reviews and approves all data applications in coordination with HDC staff.

All data are treated in accordance with all relevant federal and state statutes, including, but not limited to, FERPA (34 CFR, Part 99), HIPAA (42 U.S.C.§ 1320-d6), 42 CFR Part 2, 26 U.S. C § 6103, 42 U.S.C. § 67, 42 U.S.C. § 503, 26 U.S.C. § 3304, subpart B of 20 C.F.R. Part 603, Connecticut Student Data Privacy Act, Conn. Gen. Stat. § 10-234aa et seq., Conn. Gen. Stat. § 17a-101k(a), and Conn. Gen. Stat. § 46b-124.

B. Data Management Process

HDC has developed a secure cloud-based portal for storage and retrieval of data requested through HDC and through a data sharing agreement or contract. This portal, "Youth Services Provision" is maintained on SharePoint, separate from other CTData work files, with access restricted to CTData staff working on the HDC project. Geethika Fernando and Kate Eikel manage this portal.

Data transfer and retrieval

Unless otherwise stipulated, all HDC Project Data is acquired/transferred using Secure File Transfer Protocol. HDC project staff create a project-specific folder on the SharePoint portal. Agencies sharing data for the HDC project assign a designated staff member who will upload data to their own subfolder in the project folder. Access to the folder is limited to the point person's email address. SharePoint generates an automated email with a link to the designated staff member who can only access the folder while logged into their email. This link cannot be forwarded or used by any other users. Personnel from one agency do not have access to data supplied by other providers for the same data project or other HDC data projects on SharePoint.

After each agency's staff has uploaded their datasets for a project, HDC project staff transfer provider data to a new secure folder on the SharePoint portal for the HDC data analyst to review and integrate.

Data integration and anonymization

The HDC Data Integration Staff use standardized and replicable identity resolution strategies to integrate datasets using confidential personally identifiable data. Data providers and requesters may consult with the HDC Data Integration Staff about preferred approaches.

HDC staff develop anonymization processes for each data request. Anonymized Data is a dataset with all personal identifiers which can be used to distinguish or trace an individual's identity removed. Personal identifiers shall include those consistent with a HIPAA Limited Data Set (§ 164.514(b)(2). These include name, social security number, residential address smaller than town or city, telephone and fax

numbers, email address, Data Provider unique identifiers, vehicle or device identification numbers, web universal resource locators, internet protocol address numbers, and biometric records.

Data users sign the HDC Data Use License agreeing to the terms of receiving the data. Once data are integrated and de-identified, HDC project staff transfer the linked dataset to a separate folder on the SharePoint portal. After the data user signs the Data Use License, HDC staff grant the user access to the folder with de-identified data using their email address. The secure link cannot be shared with others.

Data retention/destruction

HDC staff retain the original data for each project until final analyses are completed.

After completion of the HDC Project (following the end of the dissemination plan), HDC project staff will store, return, or destroy Confidential Data and Anonymized Data from each Party according to the DSA(s). All data that are protected under federal and state privacy regulations will not be shared through Freedom of Information Act requests. HDC Staff will always comply with federal and state laws and will default to sharing Anonymized Data only with the approved HDC Data Recipient. The HDC Coordinator distributes a *Certification of HDC Project Completion & Destruction of Data* to require confirmation of data destruction consistent with the data use license.

C. Data Access and Security Requirements

Access and security protocols are delineated in the DSA.

Limited Access. Only HDC staff working on a specific HDC Project receive access to confidential data. Data Recipients only receive anonymized data.

Secure Storage. HDC data integration staff agree follow the requirements of *(FISM) NIST SP800-39, Managing Information Risk*. Furthermore, CTData shall be responsible for maintaining a secure environment compliant with State policies, standards and guidelines, and other Applicable Law that supports the transmission of data in compliance with the specifications.

HDC follows the security requirements contained in *(FISM) NIST SP800-47, Security Guide for Interconnecting Information Technology Systems* and employs security

safeguards contained in *(FISM) NIST SP800-53, Security and Privacy Controls for Federal Information Systems and Organizations*.

Use. HDC limits the use of confidential data solely for approved purposes. CTData limits the disclosure of confidential data to HDC project staff and Linking Hub staff for specific projects. HDC Data Integration Staff will only provide approved HDC Project Data to HDC Data Recipients who have signed the HDC Data Use License. External linking partners will review and sign confidentiality agreements prior to receiving personally identifiable information for each data project.

Data Deletion. CT Data Collaborative shall retain the Confidential Data for HDC projects for a period of twelve-months after providing the Anonymized Data to the HDC Data Recipient, unless otherwise agreed to by the Provider. After this twelve-month period, all Confidential Data and Anonymized Data will be deleted by CT Data Collaborative.

Cell Suppression Policy. CT Data Collaborative agree that HDC Projects including data from the Provider in the creation of any dissemination materials (manuscript, table, chart, study, report, presentation, etc.) must adhere to the cell size suppression policy as follows. This policy stipulates that no cell (e.g., grouping of individuals, patients, clients) with less than 15 observations may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in a cell displaying less than 15 observations. Individual level records may not be published in any form, electronic or printed. Reports and analytics must use complementary cell suppression techniques to ensure that cells with fewer than 15 observations cannot be identified by manipulating data in adjacent rows, columns or other manipulations of any combination of dissemination materials generated through HDC Projects. Examples of such data elements include, but are not limited to, geography, age groupings, sex, or birth or death dates.

Confidentiality and Breach Notification

HDC staff attached to the HDC project sign the confidentiality agreement as part of the DSA. CT Data Collaborative shall protect the Confidential Data by using the same degree of care as CT Data Collaborative uses to protect its own confidential information, and no less than a reasonable degree of care.

Breach Notification. Unless otherwise specified in a data sharing agreement, CTData is responsible and liable for any breaches of data held for an HDC data request. CTData shall report to the Data Provider all breaches that threaten the security of the databases resulting in exposure of Confidential Data protected by federal or state laws, or other incidents compromising the security of the agency's information technology systems. Such reports shall be made to the Provider within 24 hours from when discovered or should have discovered the occurrence. CTData shall also comply with any Applicable Law regarding data breaches. CTData's Cyber Liability Insurance Policy includes Breach Response.

D. Technical Security Controls

CTData's IT vendor patches CTData's managed and monitored Windows and Mac computers once per week. The managed computers are scanned daily for viruses/spyware/ransomware. Emails are protected via Exchange Online Protection, Graphus, and Microsoft's tools.