Keeping Connecticut Healthy
DPH
Connecticut Department of Public Health

Data Security and Confidentiality Policies and Procedures

2023 - 2024

TB, HIV, STD & Viral Hepatitis Section

Connecticut Department of Public Health

ct.gov/datasecurity

Rev 2/2023

Key Definitions Used in This Document

1 Personally Identifiable Information (PII)

Personally identifiable information refers to any information about an individual maintained by an agency, including: (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information linked or linkable to an individual, such as medical, educational, financial, and employment information.

3 Breach

A departure from established policies or procedures, or a compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or loss of control of personally identifiable information (PII) or protected health information (PHI). A breach is an infraction or violation of a policy, standard, obligation, or law. A breach in data security would include any unauthorized use of data, even aggregated data without names. A breach can be malicious or unintentional.

2 Protected Health Information (PHI)

Protected health information, also referred to as 'personal health information,' refers to demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and other data a healthcare professional collects to identify an individual and determine appropriate care.

4 Frequently used acronyms

CDC - Centers for Disease Control and Prevention

DSM - Data Security Manager

FOI - Freedom of Information

GIS - Geographic Information System

HIC - Human Investigations Committee

IRB - Internal Review Board

MFA - Multi-factor authentication

ORP - Overall Responsible Party

SFTP - Secure file transfer protocol

VPN - Virtual private network

CDC's 10 Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality

1. Public health data should be acquired, used, disclosed, and stored for legitimate public health purposes only.

2. Programs should collect the minimum amount of personally identifiable information necessary to conduct public health activities.

3. Programs should have strong policies to protect the privacy and security of personally identifiable data.

4. Data collection and use policies should reflect respect for the rights of individuals and community groups and minimize undue burden.

5. Programs should have policies and procedures to ensure the quality of any data they collect or use.

6. Programs have the obligation to use and disseminate summary data to relevant stakeholders in a timely manner.

7. Programs should share data for legitimate public health purposes and may establish data use agreements to facilitate sharing data.

8. Public health data should be maintained in a secure environment and transmitted through secure methods.

9. Minimize the number of persons and entities granted access to identifiable data.

10. Program officials should be active, responsible stewards of public health data.

Adapted from: Lee, LM, Gostin, LO. Ethical collection, storage, and use of public health data: a proposal for national privacy protection. JAMA 2009;302:82–84

Table of Contents

1 Introduction

Purpose
Public health surveillance data
What's New
Breach reporting
Breach investigation
Breach mitigation

5 Physical Security

Onsite
Offsite
Remote Work
Mail
Record storage
Record retention
Shredding
DPH servers
Disaster Recovery Plan

12 Data Security

Network
Server backup
Internet
Cloud computing
Desktop computers
Mobile Devices
Laptop computers
Email
Telephones
Faxing
Disposal of drives
Printing
Secure File Transfer Protocol (SFTP)
Electronic Laboratory Reporting (ELR)
Data entry
Data dissemination
Routine data requests
Data suppression
Analysis using GIS
Leave of absence
Program severance

26 Data Sharing

Local health departments
Interstate communication
National Death Index
Matching registries
Internal data sharing
Routing infectious disease surveillance reporting
Health Care and Support Services
HIV Surveillance Program data systems
Lexis Nexis
Research

32 Confidentiality Agreement

Appendices

1. CT Agency Regulation 19a-25
2. CT Agency Regulation 19a-36
3. CDC Assurances of Confidentiality
4. Section Breach Mitigation Checklist
5. HSS Breach Notification Policy
6. DPH HR Security Protocols
7. HIPAA Access Letter
8. DPH Record Retention Schedule for HIV
9. DPH Record Retention Schedule for TB & STD
10. DPH IT eHARS Servers Disaster Recovery Plan
11. eHARS Disaster Recovery Plan Table
12. HHS HIPPA Public Health Fact Sheet
13. CT OPM Network Security Policy and Procedures
14. CT OPM Policy on Security for Mobile Computing and Storage Devices
15. DAS/BITS Mobile Device Pledge
16. DPH IT Mobile Device Incident Report
17. Section Sample Fax Cover Page Disclaimer
18. NCHS Confidentiality Statute Section 308
19. DPH Data Sharing Agreement
20. DPH Severance Policies
21. 2023 Confidentiality Agreement

Other Relevant Attachments

1. DPH Confidentiality Policies and Regulations
2. DPH Confidentiality Pledge
3. DAS/BITS IT Tech Policies
4. DPH DIS Field Activities
5. CDC Security and Confidentiality Validation
6. CDC Security Assessment Checklist
7. CDC Site Visit Security Checklist

DPH Legal Office Documents

Non-HIPAA Data Security Breach Policy
Data Breach Report
DPH Breach Resolution
FOI Policy
FOI Response Template

Introduction

Purpose

This document is intended for use by TB, HIV, STD, and Viral Hepatitis Section staff and other DPH program areas which conduct public health surveillance activities and:

- describes the policies and procedures used to safeguard the confidentiality of public health surveillance data;
- is reviewed and updated annually (or as needed) by the Data Security Managers in response to changing work environments, technologies, personnel, and CDC standards;
- covers public health surveillance activities of the TB, HIV, STD and Viral Hepatitis Section and other DPH programs conducting surveillance activities and/or routinely handle personally identifying information (PII) and protected health information (PHI);
- applies to all program areas unless specifically designated.

This document is required for compliance with the CDC Data Security and Confidentiality Guidelines: *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action*, U.S. Department of Health and Human Services, Centers for Disease Control and Prevention.

These practices are considered the minimum standard. There may be scenarios not covered within this document where managers, supervisors and/or staff will need to review security and confidentiality of PII and/or PHI and may need to apply more stringent standards.

Annually and/or as needed, DPH staff with access to PII/PHI receives confidentiality training in accordance with these policies and procedures. Training is conducted by appropriate staff as determined by the Overall Responsible Party (ORP).

Public Health Surveillance Data

- Public health surveillance data are collected in accordance with Connecticut State Agency Regulations §§ 19a-25-1— 19a-25-4 and 19a-36 (Appendix 1, 2).
- Data are collected for public health purposes only.
- The minimum data are collected for the public health surveillance need.
- Information is collected, stored, and disseminated in accordance with applicable state regulation(s) and the Federal Assurance of Confidentiality (Appendix 3).

What is Public Health Surveillance ?

The ongoing, systematic collection, management, analysis, and interpretation of health-related data, followed by dissemination to other Public Health professionals in order to:

1. Monitor populations to detect unusual instances or patterns of disease, toxic exposure, or injury.
2. Activate prevention and control measures related to public health threats.
3. Intervene to promote and improve health.

WHAT'S NEW?

Remote work

Most significantly, many DPH staff have been working remotely since April 2020. Several new sections in this policy describe current processes and operations.

Microsoft Office365

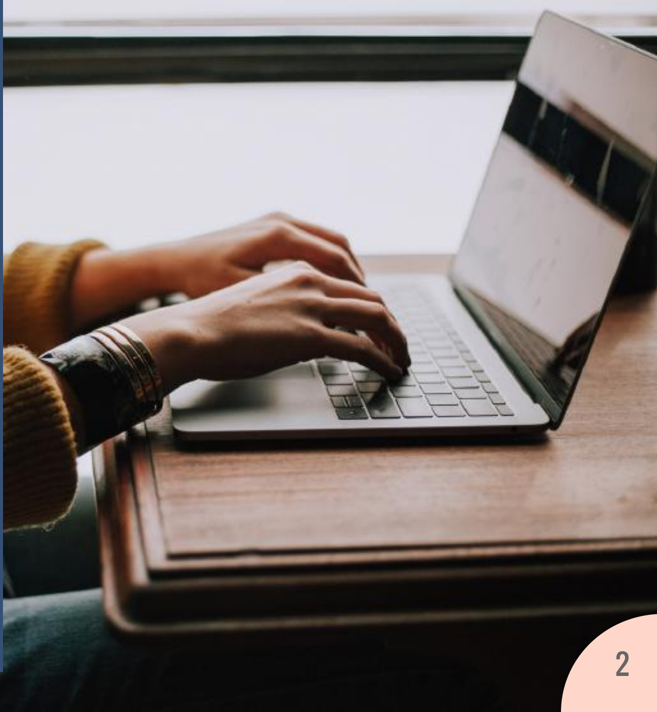
DPH has moved to secure, cloud-based Microsoft products and applications to accommodate remote work.

Breach Reporting

Data Security and Confidentiality Incident Reports are no longer necessary for breaches related to incoming e-mail containing PII or PHI. (See page 18 for details.)

Breach Investigation and Incident Reporting

Breach reporting and follow-up is standardized for all staff. There is an online incident report form to report breaches. Select Breach Response Teams are notified of incidents that may require investigation and/or mitigation activities.



Breaches Defined

There are several definitions for "breach" depending on the context. For public health surveillance data, the following definitions apply:

A breach is an infraction or violation of a policy, standard, obligation, or law. A data security breach would include any unauthorized use of data, even aggregated data without names, and can be malicious or unintentional.

A breach can also be a departure from established policies or procedures, or a compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or loss of control of personally identifiable information (PII) or protected health information (PHI).

Types of Breaches

Data Security

Any unauthorized use of PII/PHI

Protocol

Any violation of the Confidentiality Policy

Confidentiality

Any unauthorized disclosure of PII/PHI

Reporting Process

- Notify your immediate supervisor via phone, e-mail or Teams.
- Go to the CT DPH Data Security and Confidentiality Incident Report.
- Complete all sections of the report.
- "Submit."

Breach Investigation and Mitigation

Any breach of data security, protocol, or confidentiality, regardless of whether personal information was released, must be reported to your supervisor(s) as soon as possible. Breaches resulting in the release of PII/PHI to unauthorized persons must also be reported to CDC and if warranted, to law enforcement agencies.

Breach Investigation

Notification Chain

If any type of breach occurs, the first step is to notify your supervisor. The second step is to complete a Data Security and Confidentiality Incident Report. Submitted reports are received immediately by the Data Security and Confidentiality Manager(s), who then activate the Response Teams below. Response teams may vary depending on recipient(s) of PII/PHI and the number of records, patients or clients involved.

Level 1a: Exposure of PII/PHI to Unauthorized Individual(s)

Recommended team to address exposure of PII/PHI. Response teams may vary depending on recipient(s) of PII/PHI and the number of records, patients or clients involved.

- Director of Infectious Diseases (acting) - Lynn Sosa, MD
- IT Section Chief - Dennis Mitchell
- TB, HIV, STD & Viral Hepatitis Section Chief - Delores Greenlee
- Data Security Manager - Heather Linardos (HIV, Viral Hepatitis and CDC compliance)
- Data Security Manager – Alison Stratton (STD, TB and DPH compliance)
- Informatics Program Lead - Nancy Barrett
- Agency Data Officer - Gary Archambault
- Deputy State Epidemiologist - (TBD)
- DPH Legal Department Privacy Officer
- Employee Supervisor(s)
- Human Resources Advisor
- PS18-1802 Project Officers - Angela Hernandez, June Mayfield
- CDC Surveillance Data Security SME - Patricia Sweeney

Level 1b: Lost/Stolen Assets

Recommended team to address lost or stolen state-issued devices including laptops, tablets, and mobile phones.

- Director of Infectious Diseases (acting) - Lynn Sosa, MD
- TB, HIV, STD & Viral Hepatitis Section Chief - Delores Greenlee
- Data Security Manager - Heather Linardos (HIV, Viral Hepatitis and CDC compliance)
- Data Security Manager – Alison Stratton (STD, TB and DPH compliance)
- Informatics Program Lead - Nancy Barrett
- Agency Data Officer - Gary Archambault
- DPH Legal Department Privacy Officer
- Bureau of Information Technology Solutions (BITS) CIO - Mark Raymond
- IT Section Chief - Dennis Mitchell
- IT Managers - Steven McConaughy, Eva Golebiewski
- IT Data Security Officer - Nicholas Piscitelli
- Fiscal Administrative Supervisor - Daniel Velez
- Employee Supervisor(s)
- Local and/or State Police
- PS18-1802 Project Officers - Angela Hernandez, June Mayfield
- CDC HIV Surveillance Data Security SME - Patricia Sweeney

Breach Investigation

Level 2: PII/PHI Attached to E-mail

NEW

Please note, Data Security and Confidentiality Incident Reports are no longer required for incoming e-mail containing PII or PHI. (See page 18 for procedures.)

In the event of <u>outgoing</u> e-mail containing PII or PHI, the following response team will follow-up:

- TB, HIV, STD & Viral Hepatitis Section Chief - Delores Greenlee
- IT Section Chief - Dennis Mitchell
- Data Security Manager - Heather Linardos (HIV, Viral Hepatitis and CDC compliance)
- Data Security Manager – Alison Stratton (STD, TB and DPH compliance)
- Employee Supervisor(s)

(Appendix 4, 5)

Physical Security

Building

- DPH shares a multi-building complex with several other state agencies.
- State employees are required to show their agency photo ID to gain entry to the complex.
- The work area doors are locked and accessible only to employees with proximity cards.
- The TB, HIV, STD and Viral Hepatitis work areas are on the first floor with many other DPH programs.
- Visitors to the complex must sign in with Security at which point they are photographed and assigned an adhesive visitor's pass.
- Visitors are escorted while inside DPH work areas.
- See DPH Security Protocol with regard to identification badges (Appendix 6).

Workstations

- Workstations in the HIV Surveillance Program area are outfitted with 65" high panels topped with 14" glass stack-ons. Workstations also include privacy walls, locking file drawers and locking overhead cabinets.
- Individual staff are personally responsible for safeguarding confidential materials within their workstations.
- Workstation computers and or laptops must be locked when not in use or when away from desks.

Lock computers while away from your desk ⊞ + L

- File cabinets and desk drawers containing PII/PHI must be locked when staff are away from their desks.
- PII/PHI may be kept at individual workstations when needed for surveillance activities.
- Staff must take precautions to ensure that PII/PHI are not in view of unauthorized individuals.
- All monitors for workstation computers should have privacy screens. If possible, monitors should not be visible from nearby walkways.
- Work stations are checked for documents containing PII/PHI at the end of the day to assure everything has been secured in a locking desk or cabinet.

Physical Security

Off-site Workstations

- Program Coordinators grant permission for off-site work.
- Disease Intervention Specialists (DIS) are assigned work spaces in local health departments.
- Staff must be mindful that off-site workstations may be accessed by non-DPH staff or others in their absence.
- Requirements for security at off-site workstations are the same as for workstations at DPH.
- Lockable cabinets that are accessible only to DPH staff and others as assigned must be used to store PII/PHI during times when DPH staff are not present.
- Documents containing PII/PHI must be shredded or securely removed to DPH when they are no longer needed.
- Access to the DPH server from off-site offices must utilize a Virtual Private Network (VPN) or Remote Desktop Protocol (RDP). The Program supervisor will approve users for VPN access and DPH IT will assign users to a corresponding token group ID. DPH IT will provide security token devices with authentication mechanisms. Network access must be via McAfee-encrypted devices including tablet, laptop or desktop computer.
- Off-site offices must have a cross-cut shredder.
- DPH-assigned devices must be secured in a locked desk or cabinet when not in use.
- DPH staff may share PII/PHI with authorized local staff or others, as appropriate. (See Data Sharing, page 24)
- These procedures are applicable to any DPH staff located at any off-site workstation either permanently or for temporary projects.
- E-mail to and from off-site workstations must not include PII/PHI (see E-mail, page 18).

Telecommuting (Pre-COVID)

- DPH surveillance activities using PII/PHI may be conducted off-site at places of residence or alternative offices by staff approved for telecommuting.
- Supervisors will approve telecommuting for staff members who have a demonstrated ability to safeguard PII/PHI while off-site.
- After Program-level approval, staff must complete the DAS Telecommuter application.
- Telecommuters agree to:
    - use DPH-issued encrypted laptops or other DPH-issued secure, electronic mobile devices;
    - utilize secure, password protected, private internet connections/Wi-Fi to access DPH files and/or applications on the DPH network;
    - inform supervisor when using PII/PHI off-site;
    - only use the minimum PII/PHI necessary;
    - Describe how they will protect PII/PHI in their TC application.
- Paper materials or storage media in use at staff residence will be kept in a locked cabinet and returned to DPH when no longer in use.
- Locked cabinets or other secure locations will not be shared with, or accessible to, other household members.
- E-mail to and from TC workstations must not include PII/PHI (see E-mail, page 18).

Physical Security

Telework/Remote Work

- DPH staff work remotely in varying degrees depending on operational need. The current phase permits up to 80% remote. Additional remote work time is reviewed on a case-by-case basis.
- For each 6-month phase of telework, employees must apply using the link and documents shared via e-mail by Human Resources or the Commissioner.
- Supervisors and Manager can now review and approve Telework request using the : [Connecticut Department of Public Health Employee Portal](#).

Same Physical Security Rules Apply

- DPH surveillance activities or other work using PII/PHI may be conducted off-site at places of residence or alternative offices by staff approved for remote work.
- Telecommuters agree to:
  - use DPH-issued encrypted laptops or other DPH-issued secure, electronic mobile devices;
  - utilize secure, password-protected, private internet connections/Wi-Fi to access DPH files and/or applications on the DPH network via RDP or Microsoft Office365;
  - inform supervisor when using PII/PHI off-site;
  - only use the minimum PII/PHI necessary.
- Paper materials or storage media in use at staff residence will be kept in a locked cabinet and returned to DPH when no longer in use.
- Locked cabinets or other secure locations will not be shared with, or accessible to, other household members.
- E-mail to and from off-site workstations must not include PII/PHI (see E-mail, page 18).

Physical Security

Field Work

Public health field work is conducted by various DPH staff including epidemiologists, DIS, case managers and contract managers.

Data Confidentiality and Security Managers (DCSM)

- When necessary, the DCSM shall issue HIPAA access/authorization letters to staff who conduct field work.
- DCSM for HIV Programs and Viral Hepatitis: Heather Linardos
- DCSM for STD and TB Programs: Alison Stratton

(Appendix 7)

Supervisors:

- should be aware of how PII/PHI are being used in the field;
- must authorize the transport of worklists, laboratory reports or other documents that include PII/PHI in advance;
- must ensure that staff are competent in Data Security and Confidentiality practice and procedures prior to authorizing staff to conduct field work.

DPH staff working in the field will:

- take precautions to minimize risk while traveling to and from external work sites;
- carry their DPH HIPAA access letter and present it to facility or laboratory staff to verify authority to access PII/PHI on behalf of DPH;
- carry their DPH photo identification card;
- limit discussions that include PII/PHI with non-DPH staff to the minimum necessary;
- hold discussions or interviews that include PII/PHI in private;
- conduct medical record reviews where confidentiality can be assured;
- collect only the minimum of PII/PHI necessary to satisfy DPH or CDC reporting requirements;
- secure any paperwork generated from medical record reviews in locked storage until it can be returned to DPH;
- ensure that no person can access documents that include PII/PHI;
- not store PII/PHI on mobile devices or laptops;
- not record PII/PHI in calendars, planners, or notes unless indispensable for case management;
- use only password protected DPH-assigned mobile devices while in the field;
- cross-shred paper lists containing PII/PHI prior to leaving facilities;
- not leave documents with PII/PHI unattended in a vehicle.

...

Data Security Incidents in the Field

Loss of DPH-assigned devices, PII/PHI, or other breaches that occur while working in the field must be reported to the supervisor as soon as possible.

Physical Security

Paper Mail

- Program mailboxes are located inside the secure work area.
- Mail is received in US Mail or interoffice envelopes and typically delivered by 11 am.
- Clerical staff are tasked with mail pickup twice a day and delivered to program staff or stored in a specific drawer in an assigned locked file cabinet.
- Keys to the cabinets are kept in a secure area.
- Mail must be collected promptly on delivery and checked again at the end of the day.
- Mail boxes within individual program areas are secured from view.
- Envelopes containing PII/PHI are marked “CONFIDENTIAL.”
- If reports are inadvertently mailed to the wrong Program, mail must be brought to the Program it is addressed to in a sealed interoffice envelope or placed into a locked cabinet/desk if it cannot be forwarded immediately.
- Opened mail must not be left unattended in cubicles.
- Mail, both from outside sources and interoffice, addressed to any particular individual should not be opened and must be delivered to the appropriate mailbox of the person it is addressed to.
- Unprocessed mail must be stored in a locked cabinet until it can be processed.

Paper Record Storage

- When paper case reports can be archived they are moved to long-term storage in locked filing cabinets or in a designated locked room.
- Paper TB records are retained for longer periods (10 years at DPH and 11–60 years offsite). Off-site storage is at a state-owned facility in Rocky Hill. The site is visited by DPH staff but staff members at the facility are responsible for security and confidentiality.
- Paper records may be stored in the DPH long-term storage area in a locked room.
- Access to DPH locked rooms is limited to appropriate staff. Keys to the locked room are in the possession of designated staff. A master key is in the possession of physical plant staff.

HIV Locked Room

- Long-term storage of HIV paper records is in locked filing cabinets inside a locked room within a proximity card restricted area of DPH.
- The room is windowless and has one entrance.
- Access to the locked room is limited to authorized HIV Surveillance Program staff.
- A master key is in the possession of physical plant staff.

Physical Security

Record Retention

- TB, HIV, HCV and STD paper reports are retained according to the DPH retention schedule.
- Electronic records are kept in a manner consistent with the record retention schedule.

(Appendix 8, 9)

Shredding

- Paper containing PII/PHI must be shredded before disposal. If necessary, staff may use cross-cut personal shredders in cubicles for low-volume shredding jobs.
- There are three high-volume cross-cut shredders available to program staff in the following program areas: HIV Surveillance, HIV Prevention and TB-STD Program areas.
- Annual shredding is conducted by an agency-approved vendor.
- The shredding vendor (InfoShred) is used periodically to shred TB, STD and HCV papers.
- When InfoShred comes to DPH, an assigned Program staff person observes the shredding process when shredding of documents is required.
- Shredded material is re-shredded to dust when the truck returns to the InfoShred office.

DPH Servers

- DPH servers are located in one physical location at the 410 Capitol Avenue building.
- The IT work area is accessible by way of proximity cards.
- Servers are inside a secure room with one door. Access to the room is restricted exclusively to staff that hold an authorized proximity card.
- Electronic files, applications and databases reside on the virtual server environment.
- In addition to TB, HIV, STD and HCV data, DPH servers contain the electronic confidential records of many DPH programs.
- DPH IT staff are tasked with the physical security measures of servers.
- An IT staff person, with a signed current confidentiality agreement on file, is assigned to maintain eHARS and other ancillary application/databases, perform upgrades, and confer, as needed, with the HIV Surveillance Program Coordinator and/or Data Manager.

Disaster Recovery Plan (DRP)

- Instances that require restoration of Section program files, applications or databases are evaluated by the ORP and/or DSMs prior to declaration of disaster.
- The ORP will activate the DRP and coordinate with the DPH IT team for the restoration of hardware/software as required to attain normal program activities.
- Section staff will follow the actions required as set forth in the DPH IT DRP document, or as assigned, when the Disaster Recovery team requires assistance.
- The DRP document must be maintained and updated after a disaster recovery exercise reports deficiencies and/or as new technologies take place.
- The DRP document must be maintained by the ORP/DSM to reflect changes in team contact information, vendors or other critical information.

(Appendix 10, 11)

Physical Security Recap

Building

✓ DPH work area doors are locked and accessible only to employees with valid identification and proximity cards.

Workstations

✓ Computers have privacy screens and are locked when not in use. PII /PHI are locked in desk or file cabinet when not in use.

Off-site Workstations

✓ Security requirements are the same for off-site workstations. Staff must use an encrypted DPH-issued device, RPD or VPN to access DPH servers.

Telecommuting

✓ Staff who TC will inform supervisors when using PII/PHI off-site and only use the minimum necessary.

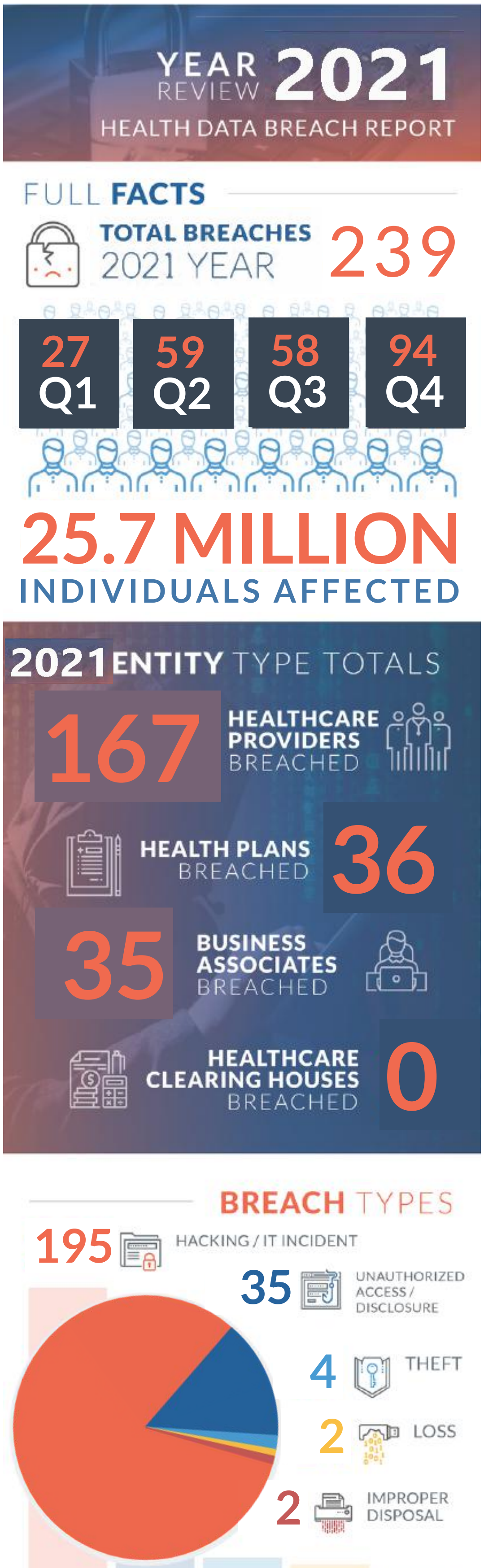
Field Work

✓ Supervisors should review the purposes for which PII/PHI are used and how they are secured when not in use.

Disaster Recovery

✓ The ORP can activate the Disaster Recovery Plan and coordinate with IT staff to restore or replace files, software or hardware lost to disasters.

Data Security



US Department of Health and Human Services, Office for Civil Rights, Breach Portal, 2021

What is Data Security?

Data security refers to the process of protecting data from unauthorized access and data corruption throughout its life cycle. Data security includes data encryption, tokenization, and key management practices that protect data across all applications and platforms.

According to the Department of Health and Human Services Office of Civil Rights, there were nearly 26 million healthcare records breached in 2021. Hacking/IT incidents accounted for 82% of data breaches and 97% of breached records.

(Appendix 12)

Although risk will NEVER BE ZERO, there are ways DPH and BITS help to avoid data security breaches.

✓ Backup and recovery

Backing up data is one of the best defenses against hackers. Ability to restore the last backup gets systems back online quickly.

✓ Security updates

DPH IT and BITS make sure that operating software is up to date as part of overall network security - alongside a robust firewall, anti-virus, spyware, and malware protection.

✓ Encryption software

DPH- assigned mobile devices come with installed encryption software which not only protects against cyber and physical data attacks, but also physical loss of data.

✓ Email vigilance

Do not open emails from senders you are not sure about. If you open a suspicious email by accident, do not click any links or open attachments!

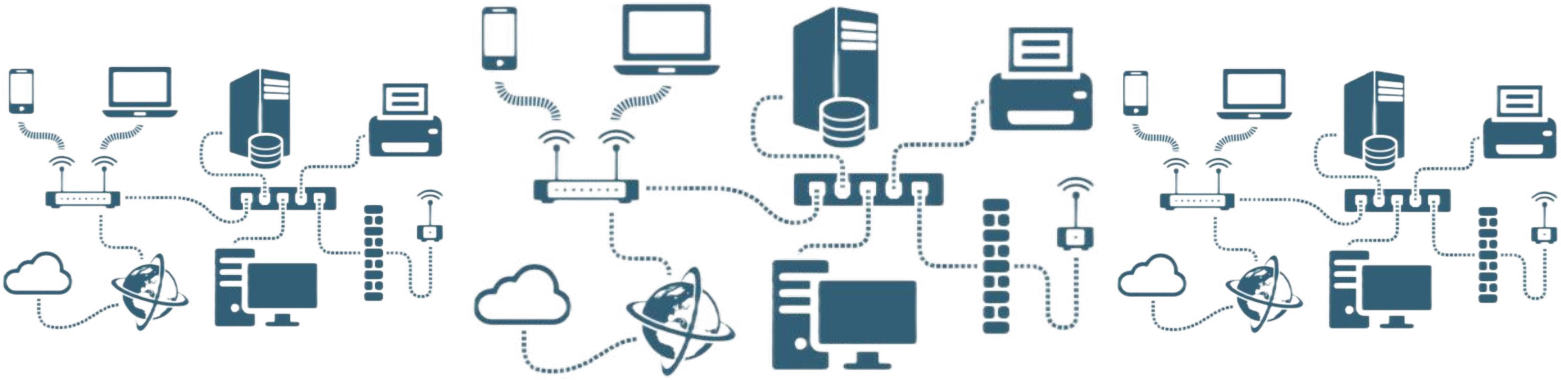
✓ Restricted access

Setting user permissions in data systems allows users access suitable for the needs for their role. This helps protect against unauthorized access to data, and ultimately may prevent a security breach.

✓ Secure Wi-Fi

DPH offers customers and guests separate Wi-Fi access to help protect sensitive data.

Data Security



Network

- Electronic files that contain PII/PHI must be stored on the appropriate Program server – not on workstation computers (unless noted in this document).
- The DPH IT network administrator, with approval of the ORP, assigns server access rights. Access rights are assigned on a need-to-know basis and are reviewed periodically. The DPH network and servers are protected by a firewall.
- Before network access is granted, staff members receive Data Security and Confidentiality training and sign the Confidentiality Agreement.
- The DPH network, servers, and computers are protected by McAfee VirusScan.
- DPH inbound and outbound network traffic is monitored by BITS for suspicious packages and potential intrusions. DPH staff monitor this traffic as needed using ISS IBM Proventia Site Protection System.
- DPH network access is restricted by User ID.
- Monitoring logs are kept to record the network activities of each Machine ID/Mac Authentication through a network monitoring tool.
- The DPH IT Security Officer is Nicholas Piscitelli.
- DPH IT continually upgrades the data security environment in response to evolving technology and potential security threats.
- The network is sub-netted and divided into VLANs to reduce access to unapproved restricted sources.
- DPH IT monitors Federal, State and vendor alerts regarding threats and vulnerabilities, assesses the risk and applies the appropriate remediation.
- DPH IT is continually improving the Agency's network and security infrastructure.

(Appendix 13)

Data Security

Server Back-up

- An encrypted tape back-up copy of DPH server content is made daily and stored in the IT area on the 3rd floor of the 410 building. A backup tape is sent off-site to a private company weekly.
- Back-ups of all DPH and BITS servers run nightly.
- Servers are backed up to an attached Arcserve UDP Appliance on a nightly basis. The data is then backed up to tape on a Dell PowerVault TL400 to send offsite.
- Data is encrypted using 256bit AES (Advanced Encryption Standard) scheme before being added to the tape.
- Off-site storage: William B. Meyer | Records Management, Windsor, CT.
- Recovery of information from back-up tapes is not possible without highly specialized software, equipment, and skills.
- Use of back-up copies to restore files is requested through the appropriate DPH staff and network administrator.
- When data file(s) /directory/application restoring is required, the ORP/DSM will follow procedures as described in the *Server Data Backup Procedures* document, which is maintained by DPH IT.

Internet

- All workstation computers have access to the internet with 128-bit cipher strength.

Data Security

NEW

Microsoft Azure

Office 365

Cloud Computing

- DPH IT rapidly deployed cloud-based Microsoft365 to enable remote work in response to the COVID-19 pandemic in March-April 2020.
- Microsoft365 requires re-authentication every 7 days.
- Within Microsoft365, DPH staff can access the full Office Suite including Word, Excel, PowerPoint, Outlook, Teams, Forms, OneNote, and OneDrive.

Staff working remotely can communicate with other staff using Teams. Staff utilize the chat feature, conduct video calls, and schedule meetings.

Many DPH VPN users have moved to Remote Desktop Protocol, which enables remote access to a workstation desktop computer and DPH applications, secure drives, files, and servers.

DPH IT has created access to many Program-specific applications utilizing Azure Active Directory's Application Proxy, which provides secure remote access to on-premises web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal application portal.

Q & A: Communicating PII/PHI via Office365 Apps

Can DPH staff use Teams to discuss case information that includes PII/PHI?

Yes. Staff can conduct confidential case discussions via Teams provided they have a private area office or remote work locations to do so.

Can DPH staff use Microsoft cloud-based apps (Teams, OneDrive) to share PII/PHI, when necessary?

Yes. Network communications **are encrypted by default**. By requiring servers to use certificates and by using OAUTH, Transport Layer Security (TLS), and Secure Real-Time Transport Protocol (SRTP), all data are protected on the network.

Data Security

Desktop Computers

- A user-ID/password is required to gain access to workstation computers and to the DPH network.
- Password changes are required every 60 days.
- CT DPH complies with the Federal Social Security Administration of the Active Directory password policy by maintaining current password standards.
- Workstation computers must have password-protected screensavers.

Creating a Screen Saver with Password in Windows 10

1. Click on the Windows icon in the banner on the lower left corner of your display
2. Click the gear icon above the power button
3. Click **Personalization**
4. From the left menu, click **Lock screen**
5. In the Lock screen window, click **Screen saver settings** at the bottom
6. Choose a screensaver, choose a time after which it will come on, and check the box **On resume display log-in screen**
7. Click **OK**
8. The log-in will ask you for your current password

- Workstation computer hard-drives must not contain PII/PHI.
- Staff must lock their computer when they are away from their computers and log-off the network at the end of each workday.
- To lock the computer press the <ctrl+alt+delete> or <⊞+ L> keys at the same time.

Devices

With regard to data security, the following are defined as storage devices:

- USB flash drives, external drives, and SD cards.

The following are defined as mobile devices:

- Laptops, notebooks, iPads, tablets, mobile phones, smart watches, or any device with photographic/storage capability.

Use of Storage or Mobile Devices

- Users of storage and/or portable devices must be in compliance with current CT state policy on security for mobile computing and storage devices.
- With authorization from immediate supervisor, users must complete the 'IT Mobile Data Control' form.
- Personal phones, tablets, or other unspecified devices must not be used to access, record, photograph, or transport PII/PHI.
- USB drives or other stand-alone hard drives that are DPH property may be used as a temporary transport device but must be encrypted.
- PII/PHI must not be left on these devices longer than is necessary.
- DPH storage or mobile devices must be secured in a locked drawer when not in use.
- Portable devices must not be left unattended in a vehicle.

(Appendix 14, 15, 16)

Laptop Computers

- All DPH laptops are required to have current DPH encryption software.
- After six months without update, laptops become inaccessible.
- Laptops are encrypted with a National Institute of Standards and Technology (NIST) certified encryption algorithm, AES FIPS 256 compliant, cannot be bypassed by the user, and fully encrypts all files on the hard drive including operating system files.
- Case information is not collected directly into laptops and registries are not installed on laptops.
- Use of laptops for case management purposes must be approved by the supervisor and/or Program Coordinator.
- DPH laptops that have been encrypted by DPH IT staff may be used for daily work that does not include PII/PHI.
- Telecommuters are authorized to use encrypted DPH laptops.
- Staff may use encrypted DPH laptops at authorized offsite workstations.
- At the end of each day, laptops must be completely shut down and powered off. Do not leave a laptop in "sleep" or "stand-by" mode.
- If returning to DPH or field office at the end of the day, bring the laptop to your workstation and lock in a file drawer.
- If not returning to your official workstation at the end of the day, bring the laptop inside your home and store in a secure area such as a locking file cabinet.
- Never leave a DPH laptop or tablet unattended in a vehicle.

E-mail

- State e-mail can become publicly available under the Freedom of Information Act.
- Work e-mail is not private and copies reside on administrative servers and backups.
- Except as described below, e-mail to DPH staff or to addressees outside DPH is not used to transmit PII/PHI or attach files (including encrypted files) containing PII/PHI. This applies to use of the DPH e-mail system from inside DPH or external use via internet access of DPH e-mail.
- E-mail must include an automatic signature block stating that e-mail must not be used to transmit PII/PHI.
- To setup automatic signature in MS Outlook go to File ->Options ->Mail ->Signatures.

E-mail Signature Template

Please do not respond to this e-mail with any personally identifiable information (PII) or protected health information (PHI). This includes but is not limited to name, phone number, address, date of birth and medical record number. If you need to relay or exchange PII/PHI, please contact me by phone. Thank you.

If e-mail is received with PII/PHI from any source, including clients who identify as positive for HIV, TB, HCV or an STD, the following steps must be taken:

1. Delete the e-mail containing the PII/PHI.
2. If responding to the e-mail, delete the PII/PHI prior to sending.
3. Remind the sender not to send PII/PHI through e-mail as DPH e-mail is not secure or encrypted and ask that the e-mail with the PII/PHI be deleted from all e-mail folders (including sent and deleted folders).
4. Notify your supervisor and DSC Manager for your program of the incident.

MailGate

- Assigned staff use MailGate e-mail as a DPH-approved method for transmitting confidential information.
- This system is used by DPH staff when communicating with health care providers and others regarding public health follow-up of clients and cases where transmission of confidential information is critical to the care of the patient.
- Staff may also use secure e-mail systems initiated by another person sending an e-mail to the DPH staff member from outside of the state e-mail server.
- This includes secure messages received from hospital systems that require additional login credentials or are labeled “secure” in the subject line.
- Even when using secure e-mail systems, PII/PHI should be kept to the minimum necessary to communicate necessary information.

Telephone Communication

- Telephone communication of PII/PHI is made only to authorized individuals. When in doubt, obtain a call-back number and call the person back to assure it is an appropriate person receiving the confidential information. The phone number can also be searched on the internet to determine where the call is coming from.
- CDC posts contact information of staff in other states conducting surveillance. Surveillance program staff can obtain a copy of the posting from CDC’s portal (SAMS, SharePoint) when communicating with surveillance staff in other states.
- Telephone conversations are conducted in program workstations and minimizing the use of names. Staff must be aware that cubicle configuration is not optimal for conducting confidential conversations. Every effort must be made to protect confidentiality of case/client information.
- PII/PHI are not left in non-DPH voice-mail unless known to be confidential and is so stated in the destination voice message. DPH voicemail is password-protected and thus confidential. DPH voicemail greetings should include that voice mailboxes are confidential.
- Text messages must not contain PII/PHI. Texted communications should only include necessary information with efforts made to discuss confidential information over the phone or in person.

Facsimile Communication

- DPH utilizes RightFax to receive information containing PII/PHI. RightFax supports compliance with HIPAA privacy and security rules by digitizing paper-based protected health information for private, secure and auditable electronic distribution.
- Traditional faxes may be used to send PII/PHI to laboratories or medical providers when rapid transfer is necessary.
- Disease-specific references (HIV, AIDS, CD4, Syphilis, Hepatitis C, etc., or related terminology) must not be included in the content and/or fax cover page.
- The sender should ensure that the fax number is correctly entered and contact the person receiving the fax by phone prior to sending the fax.
- The fax cover page must include a disclaimer (Appendix 17).
- Fax users must notify their supervisor if a fax number is misdialed.
- The fax machine must be checked each night to ensure that PII/PHI are not left in the tray.

Disposal of Hard Drives

- Computer, laptop and server hard drives scheduled for retirement are separated from the computer chassis and degaussed.
- When DPH copiers or fax machines are replaced, an approved vendor technician will remove the drive and turn it over to IT to be destroyed or erased.
- Document Center hard drives are encrypted.

Disposal of USB Drives

- USB drives used to transport PII or PHI must be cleared after use.
- EaseUs Partition Master is used to delete and remove existing data on USB drives.
- After processing, data is permanently deleted and the device is permanently disabled.

Printing

- Printing work lists that contain PII or PHI requires supervisor approval. This includes comprehensive lists of cases for specific facilities or other lists containing PII/PHI.
- Confidential print jobs must be sent to a printer within a Program cubicle.
- The centralized printer may also be used as an alternative. To ensure that confidential files are not printed out at the centralized printer unattended, all (confidential and non-confidential) print jobs to the centralized printers must be password protected.

Secure File Transfer Protocol (SFTP)

- Staff that needs to exchange PII/PHI with non-DPH entities may use a secure FTP connection to upload or download files.
- The IT Supervisor will determine DPH-user server or client role in the data transfer protocol.
- Notify the DSC Manager when SFTP account is activated.
- Files should be encrypted prior to posting in the client/server architecture.
- Passphrase or public keys can be exchanged via e-mail or by phone.

Electronic Laboratory Reporting (ELR)

- **ELR is in place at DPH for electronically reporting laboratory findings.** The capabilities are continually changing as laboratories transition to electronic communication with DPH. This section of the Policy and Procedures will be updated as the system matures and requirements evolve to reflect the status of security and confidentiality measures required for compliance.
- Currently electronic file transmission of laboratory reports are classified as HIPAA-covered information. As such, they are handled in compliance with the prescribed encryption standards and transmitted only over secured communications channels.
- Electronic files and documents containing laboratory results may be received in many file formats and all documents are transmitted through secured communications links and stored in file systems that meet current HIPAA requirements.
- The accepted methods of transmitting files to DPH are:
  - State-managed SFTP through ct.gov;
  - The CDC administered Public Health Information Network (PHIN-MS);
  - DAS/BITS managed B2B VPN connections between corporate end points (most appropriate for hospitals or Connecticut-based laboratory installations);
  - Token-based VPN authentication managed through DAS-BITS issued tokens;
  - E-mail is not a permitted method to exchange result files.
- Reporting parties who are not able to use an electronic delivery method have the option to encrypt or password-protect the file containing lab results and save to an a USB FIPS 140-2 compliant encrypted flash drive and delivering the drive and its contents to DPH personnel. Mailing of USB flash drives must follow directives described in the 'Mail' section of this document. A password will be provided to the recipient using a different method (usually e-mail or phone call).

Electronic laboratory reporting (ELR) (continued)

- Any HIPAA-classified data being loaded onto a portable device (USB device, external drive, laptop, etc.) must use a FIPS 140-2 compliant encryption and conform to the State Mobile Device Policy (Appendix 14).
- Upon arrival to the agency, DPH staff must relocate the file to a secure location within the agency network. DPH staff must remove the files from the portable devices and ensure that all copies are erased.

Data Entry

- Case report data are entered only into the approved surveillance registry.
- If visitors enter the cubicle when data are being entered, the monitor must be turned off and PII/PHI shielded from view. Staff must logoff the network and lock any PII/PHI in file cabinets when leaving their workstation.

Data Dissemination

- Standard tables and graphs are released annually on the DPH website.
- Non-routine data requests are considered at any time.

Routine Data Requests

- Requests for data analysis must be approved by the appropriate Program Coordinator, Section Chief and once approved, referred to the appropriate Data Manager.
- Data subsets (data sets) from the registry used for analysis must include only the minimum elements necessary and must not include PII/PHI.
- Data sets must be encrypted or deleted when not in use and stored in assigned Program's secure server domain(s).
- Data sets are not permitted to be stored on workstation computer hard drives, laptops, USB drives, or on unauthorized server domains.
- Data sets are not shared via e-mail.
- Analysis products must be approved by the appropriate Program Coordinator and Section Chief before being sent to the data customer. Output must not contain cell sizes <5.

Data Suppression

- Data Managers and staff involved in data analysis and reporting must be appropriately trained in the use of PII/PHI in data analysis.
- Aggregate data tables are available at the state, county, town/city and census tract. In general, the census tract is the smallest geographic unit of analysis (total population at least 1,500) but information for any geographic unit may not be released if there are concerns about low cell size or small numerators/denominators.
- Tables resulting in cell sizes of five or less are evaluated on a case-by-case basis to ensure the data are not identifying, especially when releasing data by town or census tract. For example, tables with cell sizes of one, where that individual may appear in more than one demographic or risk category (e.g., Asian, MSM, >50 years, resident of [town]), are not released.
- In the calculation and release of rates, care must be taken where the numerator and/or denominator are small or if the difference between the numerator and denominator is small. Typically, release of information about a specific demographic subgroup in a geographic area requires a numerator of at least 5 and a denominator of at least 100;
- Output where the numerator or denominator is small and approaching the limits above must be discussed with the Program Coordinator to determine if release is warranted and appropriate.
- Analysts must always use caution regarding the following analysis categories when cross tabulating to prevent inadvertent identification:
  - infrequent race/ethnicity categories such as Native Hawaiian/Other Pacific Islander;
  - transgender or other infrequent gender categories;
  - small or single-year age groups;
  - small or single-year race groups;
  - small geographic areas.
- When the analysis product is complete and ready to share with the requestor, data managers share with program supervisor and manager for final approval.
- CDC release of Connecticut HIV surveillance data conforms with the current data release agreement between CT DPH and CDC (available on request).

Geographic Information System (GIS) Analysis

- If PII/PHI is used in GIS analysis, precautions must be taken to protect confidentiality.
- Addresses and their equivalent latitudes and longitudes are identifiers and must be safeguarded using the same methods used to safeguard names.
- Data sets used for GIS analysis must be kept in the appropriate HIV Surveillance Program server domain behind the DPH firewall.
- Encryption must be used whenever possible.
- Results of GIS analysis must not be released in the form of spot maps (where single cases are represented as dots) or other maps that could be identifying.
- Care must be taken that use of demographic (age, race, gender) or behavioral subsets (MSM, IDU), which may be used to select cases for analysis, does not lead to identification.

Leaves of Absence

- DPH staff on leave for >45 days are temporarily disabled from network access per IT policy.

Program Severance

- Section staff who retire, are terminated, resign from DPH, or change jobs within DPH (outside of the Section) are not authorized to access or utilize PII/PHI contained in any data system within DPH.
- The DPH Help Desk must be contacted to revoke access to secure drives, the sFTP and wipe VPN drive mapping.
- Program Coordinators must revoke access to ancillary data bases and systems on the employee's last day.
- The respective CDC Project Officers must be alerted that the person is no longer a member of the CT DPH Section/Program and must revoke access to SAMS, SharePoint, CDC e-mail listservs, and any other access privileges assigned by CDC.
- Electronic devices and/or data storage devices that may contain PII/PHI must be collected prior to the employee’s last day.

(Appendix 20)

Data Security Recap

Desktop Computers

Workstation computer drives must not contain PII/PHI and staff must lock their computer when away from their desks.

Mobile Devices

Personal phones, tablets, or other unspecified devices must not be used to access, record, photograph, or transport PII/PHI.

E-mail

E-mail to DPH staff or to addressees outside DPH cannot be used to transmit PII/PHI.

Data Suppression

Tables resulting in cell sizes of five or less are evaluated to ensure data are not identifying.

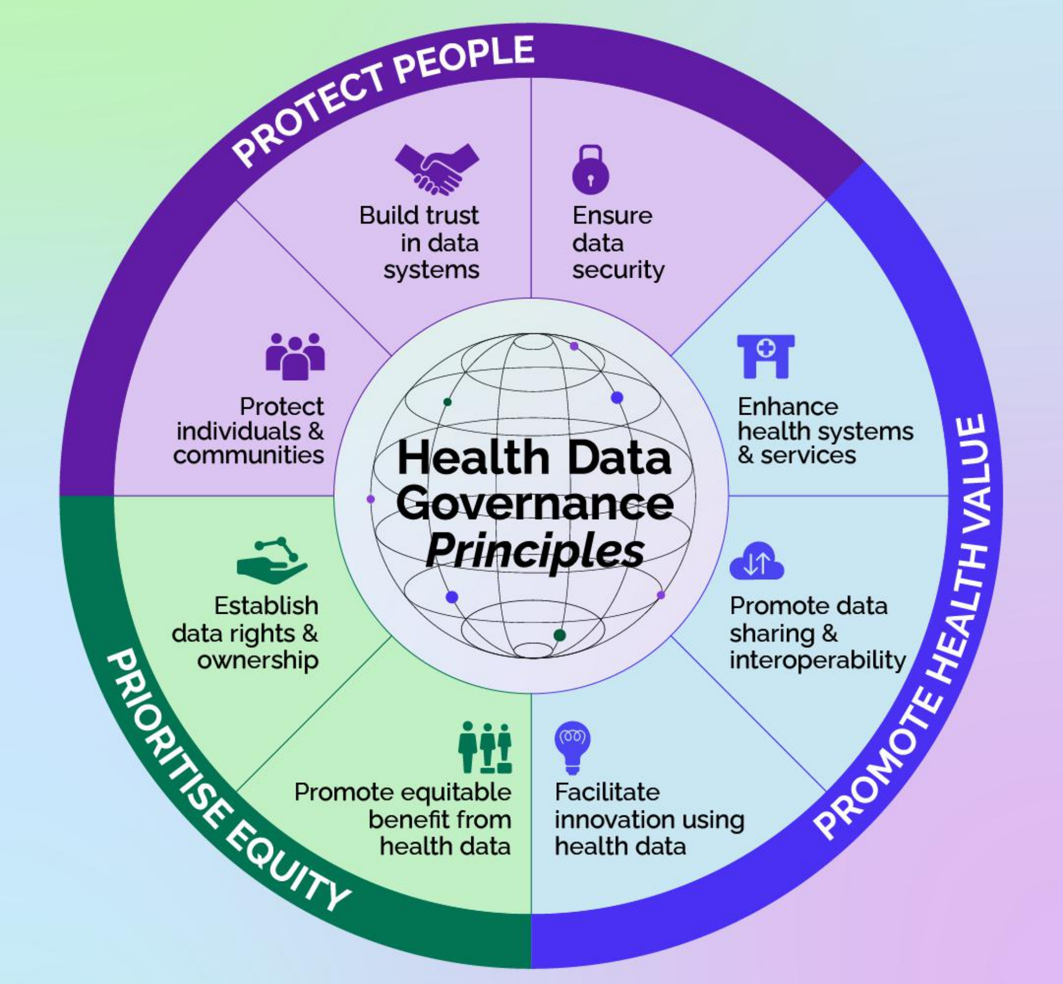
Data Entry

PII/PHI must be shielded from view when visitors enter workstations. Staff must logoff the network and lock any PII/PHI in file cabinets when leaving their workstation.

Program Severance

DPH staff who retire, resign, or are terminated are not authorized to access or utilize PII/PHI contained in any data system within DPH.

Data Sharing


PROTECT PEOPLE
Build trust in data systems
Ensure data security
Protect individuals & communities
Health Data Governance Principles
Enhance health systems & services
Promote data sharing & interoperability
Establish data rights & ownership
Promote equitable benefit from health data
Facilitate innovation using health data
PRIORITISE EQUITY
PROMOTE HEALTH VALUE

Sharing PII/PHI

- PII/PHI are not released except in situations where public health need is compelling, control over confidentiality assured, and when not specifically prohibited by statute.
- Permission of the Program Coordinator is needed to release PII/PHI. ORP permission is sometimes needed.
- Only the minimum necessary PII/PHI are shared or released.
- Expanded CDC guidance related to data sharing and data governance is in development.
- Current data sharing scenarios and permissible uses are detailed in this section.

Local Health Departments (LHD)

- HIV: HIV is not reportable to LHDs. However, an option exists for LHD to receive HIV surveillance data for public health purposes. To do so, the Director of Health must provide a protocol and an "Assurance of Confidentiality" for approval by the Program Coordinator and ORP. An Assurance of Confidentiality is defined as a guarantee under 308(d) of the Public Health Service Act that identifying information provided by the surveillance system will be held in confidence, will be used only for the purposes stated in the assurance, and will not otherwise be disclosed without the consent of the individual. (Appendix 18) (https://www.cdc.gov/rdc/Data/b4/section308.pdf)
- Sexually Transmitted Diseases: STDs are reportable to LHD. The STD Program may communicate case information to LHD, as needed, for implementation of local control measures.
- TB: TB is reportable to LHD. TB Control Program staff may communicate case information to LHD, as needed, for implementation of local control measures. TB/HIV co-infection may also be reported to LHD.
- Hepatitis C: Hepatitis C is reportable to LHD. The Integrated Viral Hepatitis Surveillance and Prevention Program may communicate information to LHD, as needed, for implementation of local control measures.

Inter-state HIV Surveillance Program Communication

- Designated staff working in HIV surveillance programs in other jurisdictions may be contacted to complete case information, establish residency, and conduct duplicate reviews to satisfy PS18-1802 grant requirements.

National Death Index

- National Death Index data is used to match with the HIV Surveillance Registry to determine vital status. Encrypted HIV data are sent to the National Center for Health Statistics for matching.
- Potential matches are reported back to DPH for evaluation.

Data Sharing

Matching Registries

- All files used for matching must comply with secure transport requirements before its availability for the actual matching process.
- All files used for matching must be located behind DPH firewall and under the restricted-access directory of a Section Program.
- Matching must be conducted by Section staff, within DPH, using DPH-provided or approved software. A variety of matching programs are available for use.
- Files used in matching are encrypted or deleted when not in use.
- Matching between HIV and Vital Records to ascertain perinatal exposure cases and vital status is conducted monthly.
- Matching between hepatitis C and HIV occurs periodically to characterize co-infected cases.
- Matching between HIV and STD occurs when requested to characterize co-infected cases.
- Matching between TB and HIV occurs quarterly to identify HIV-positive cases and update case status from HIV to AIDS for co-infected cases.

Internal Data Sharing

- DPH data sharing policy allows for DPH Programs to request data from other Programs for public health use.
- A form is available that must be approved by the appropriate program coordinators and managers (Appendix 19).
- Programs within the same Sections are administratively combined and do not need to use the data sharing form however, Program Coordinators may wish to utilize an internal data sharing agreement to document the purpose, details and frequency of the data exchange (Appendix 19).

Routine Infectious Diseases Surveillance Data Reporting

- Routine HIV surveillance data are reported monthly using CDC Secure Access Management Services (SAMS).
- STD, TB and hepatitis C data are reported to CDC using the National Notifiable Diseases Surveillance System (NNDSS).

Health Care and Support Services (HCSS)

- HCSS is a HIPAA entity and must abide by HIPAA Provider policies and regulations.
- HCSS stores electronic historical client data (Part B) on a secure server at DPH. Only HCSS and IT staff have access to the HCSS server.
- HRSA Part B client records are kept electronically as of 2020 and CT AIDS Drug Assistance Program (CADAP) since 2019.
- Both are managed by business associates: RDE (e2CT) for Part B clients and Magellan for CADAP.
- PHI/PII are suppressed to RDE. Magellan is authorized for full client data access.
- Access to HCSS data systems is limited to program staff and appropriate contractors.
- Data-to-Care staff funded through HCSS may also have access to these databases.
- Per 19a-25, it is permissible for HCSS to release PHI/PII to HIV Surveillance Program staff without an individual's consent. Any PHI/PII released from HCSS must be documented by
    - Staff and Program requesting the information;
    - Justification for release of information without consent;
    - Type of PHI/PII released (name, DOB, etc);
    - Date and time the information was accessed or shared.

- A Data Sharing Agreement between HCSS and HIV Surveillance may be executed to facilitate exchange of information provided that:
    - Only individuals named on the data sharing agreement may review the PHI/PII exchanged;
    - Only the data elements outlined in the agreement are exchanged;
    - Additional information requested outside the data sharing agreement must be document as outlined above;
    - Date and time the information was accessed or shared is documented.

Data Sharing

HIV Surveillance Program Data Systems

HANK (HIV-AIDS Networked Knowledgebase)

- When necessary, access to HANK is granted to Infectious Diseases Section staff for case investigation purposes.
- Staff with access to HANK are assigned to user groups where feature access is restricted to minimum PII/PHI necessary for specific work needs.
- Users are trained to navigate the system by HIV Surveillance Program staff.

eHARS (National HIV/AIDS Reporting System)

- When necessary, read-only, front-end eHARS access is granted to TB, HIV, STD, and/or Viral Hepatitis staff for case investigation purposes.
- Staff with access to eHARS are trained to navigate the system by HIV Surveillance staff.
- Access to eHARS datasets, files, or folders is restricted to HIV Surveillance staff and/or staff authorized by the Program Coordinator, Section Chief and Branch Chief.

LexisNexis

- The DPH Lexis Nexis account administrator is Jennifer Vargas (HIV Surveillance Program).
- LexisNexis® Accurint is used to ascertain additional information about reported cases including address, alias names, vital status, and contact information.
- Authorized DPH staff conduct searches. User IP addresses are translated into a generalized DPH IP address when the search request exits the DPH network.

Research

- PII/PHI may be used for research when Institutional Review Board (IRB) and Human Investigations Committee (HIC) approvals have been obtained.
- Research may be internal to DPH or external.
- Appropriate Program Coordinator and ORP approval is required.
- Consent of the cases or subjects may be required.
- Research that does not involve PII/PHI must still be reviewed and approved by the IRB/HIC Chair.
- Letters of support to external entities require Section and Branch Chief approval.

Data Sharing Recap

PII/PHI

PII/PHI are not released except in situations where public health need is compelling, control over confidentiality assured, and when not prohibited by statute.

Minimum Necessary

Every effort is made to limit the disclosure of PII/PHI to the minimal amount necessary to accomplish the public health purpose.

Matching

Matching must be conducted by Section staff, within DPH, using DPH-provided or approved software.

Internal Data Sharing

DPH Programs can request data from other Programs for public health use by utilizing a Data Sharing Agreement.

Health Care & Support Services

HCSS is a HIPAA entity and must abide by HIPAA Provider policies and regulations. HRSA data in HCSS systems are managed by business associates.

Research

PII/PHI may be used for research when Institutional Review Board (IRB) and Human Investigations Committee (HIC) approvals have been obtained.

Confidentiality Agreement

You have reached the end of this document.
Please take a moment to review appendices and attachments.

The next step in the Data Security and Confidentiality training process is to sign and submit a Confidentiality Agreement.

(Appendix 21)

Confidentiality Agreements are reviewed, signed and submitted via Survey Monkey.

Click here to complete the Confidentiality Agreement

Thank you!