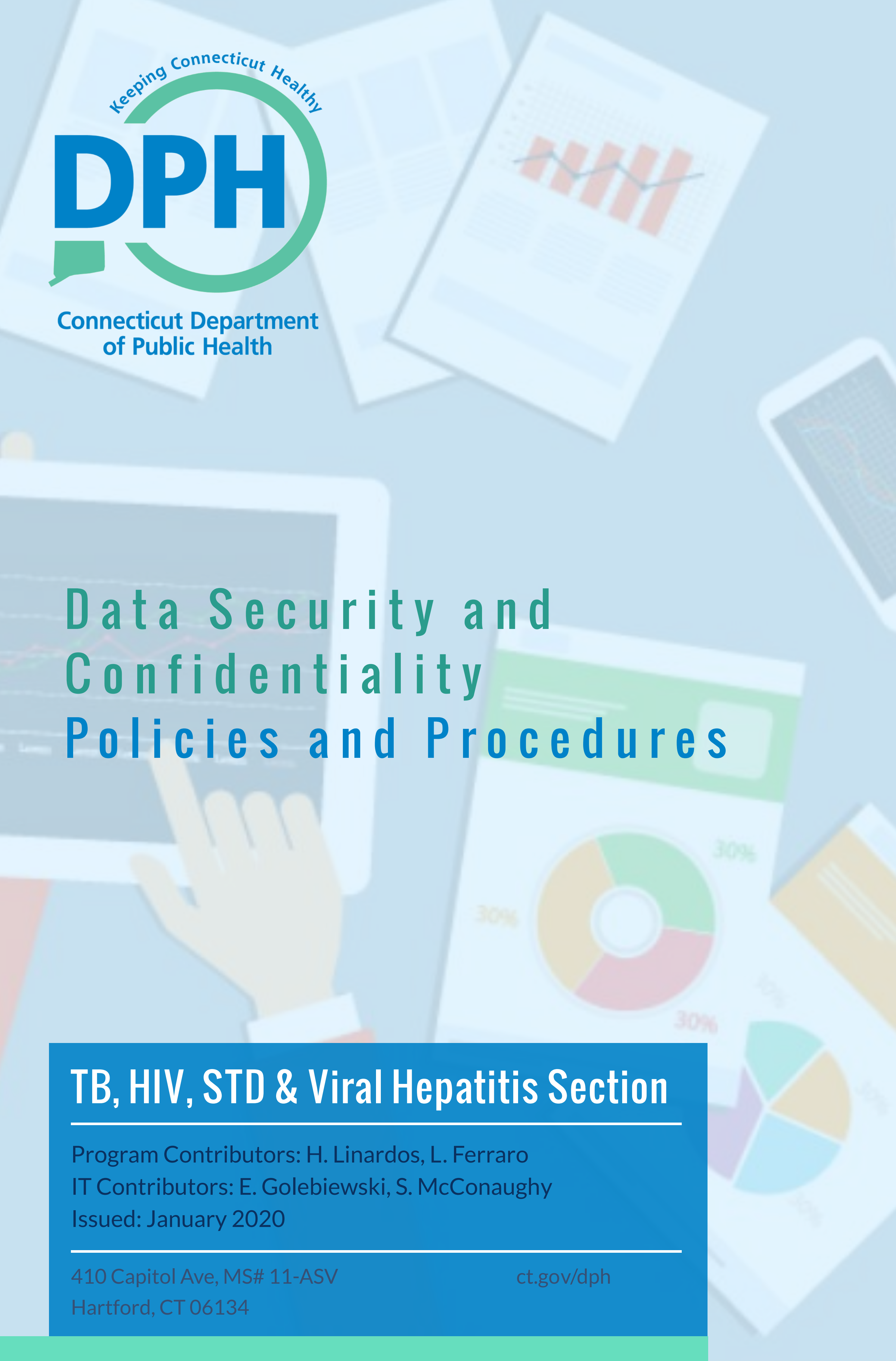


Keeping Connecticut Healthy

DPH

Connecticut Department
of Public Health

Data Security and Confidentiality Policies and Procedures

TB, HIV, STD & Viral Hepatitis Section

Program Contributors: H. Linardos, L. Ferraro
IT Contributors: E. Golebiewski, S. McConaughy

Issued: January 2020

410 Capitol Ave, MS# 11-ASV
Hartford, CT 06134

ct.gov/dph

Rev 2/2020

Table of Contents

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 that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

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 that a healthcare professional collects to identify an individual and determine appropriate care.

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.

4 Frequently used acronyms

CDC - Centers for Disease Control and Prevention
DSM - Data Security Manager
ORP - Overall Responsible Party
PGP - "Pretty good protection" encryption software
sFTP - secure file transfer protocol
VPN - virtual private network
HIC - Human Investigations Committee
IRB - Internal Review Board
FOI - Freedom of Information
GIS - Geographic Information System

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

WHAT'S NEW IN 2020?

Breach Reporting

Breaches of any kind can be reported using this form. If a breach occurs, notify your supervisor, then report the breach online. This form will be forwarded to DPH Privacy Officer for follow-up, if necessary.

DPH Legal Department

Please review the DPH Legal Department documents regarding breach reporting to the Agency and Freedom of Information requests .

Data Security Managers

Heather Linardos for HIV Programs (PS18-1802 grant requirements), and HCV/CDC compliance.

Linda Ferraro for STD and TB Programs/DPH compliance.

Breach Investigation and Incident Reporting

To best protect the Agency and staff involved in breaches, breach reporting and follow-up has been standardized to include an online report form, Response Teams and a structured checklist for investigation and mitigation.

Introduction

Public Health Surveillance Data

- TB, HIV, STD and hepatitis C (HCV) surveillance data are collected in accordance with Connecticut Agency Regulations 19a-25 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 and the Federal Assurance of Confidentiality (Appendix 3).

Confidentiality Policy

The DPH Data Security and Confidentiality Policy and Procedures for the TB, HIV, STD, and Viral Hepatitis Section:

- Describe the policies and standard procedures used to safeguard the confidentiality of public health surveillance information;
- Are reviewed and updated annually or as needed by the Data Security Managers (DSM) in response to changing technologies, personnel, and CDC standards;
- Cover CDC-funded activities of the TB, HIV, STD and HCV programs. Program-specific guidelines will be labeled (e.g., HIV is not reportable to local health departments). Components that are not specifically labeled apply to all program areas.

This DPH policy is intended to be in 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.

This DPH policy is considered the minimum standard. There may be scenarios not covered within this policy where staff, supervisors and/or Program Coordinators will need to exercise good judgment about security and confidentiality of personally identifying information (PII) and protected health information (PHI) and may need to apply more stringent standards. Annually and as needed, 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).

What is public health surveillance ?

The ongoing, systematic collection, management, analysis, and interpretation of health-related data followed by their dissemination to those who need to know in order to:

1. Monitor populations to detect unusual instances or patterns of disease, toxic exposure,or injury;
2. Act to prevent or control these threats;
3. Intervene to promote and improve health.

What is a Breach?

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 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
- Notify ORP (Heidi Jenkins)
- Go to the CT DPH Data Security and Confidentiality Incident Report
- Complete all sections of the report
- Click "Submit"

Breach Investigation and Mitigation

Any breach of data security, protocol, or confidentiality, regardless of whether personal information was released, must be reported to the ORP, DSMs, and supervisor(s) for immediate investigation. Breaches that result in the release of PII/PHI to unauthorized persons must also be reported to CDC and if warranted, to law enforcement agencies.

32%
of data breaches
involve phishing

Breach Investigation

Any breach of data security protocol, regardless of whether personal information was released, must be reported to the ORP for immediate investigation. Breaches that result in the release of PII/PHI to unauthorized persons must also be reported to CDC and if warranted, to law enforcement agencies.

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/clients involved.

- PS18-1802 Overall Responsible Party - Heidi Jenkins
- PS18-1802 Data Security Manager - Heather Linardos
- TB/STD Data Security Manager – Linda Ferraro
- PS18-1802 Project Officers - Angela Hernandez, Magan Pearson
- CDC Data Security Consultant - Patricia Sweeney
- Employee Supervisor(s)
- Human Resources Advisor - Theresa Seabrook
- DPH Legal Department
- State Epidemiologist - Matthew Cartter, MD
- Deputy State Epidemiologist - Lynn Sosa, MD

Level 1b: Lost/Stolen Assets

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

- PS18-1802 Overall Responsible Party - Heidi Jenkins
- PS18-1802 Data Security Manager - Heather Linardos
- TB/STD Data Security Manager – Linda Ferraro
- PS18-1802 Project Officers - Angela Hernandez, Magan Pearson
- CDC Data Security Consultant - Patricia Sweeney
- Employee Supervisor(s)
- Human Resources Advisor - Theresa Seabrook
- DPH Legal Department
- State Epidemiologist - Matthew Cartter, MD
- Deputy State Epidemiologist - Lynn Sosa, MD
- IT Supervisors - Steven McConaughy, Eva Golebiewski
- IT Data Security Officer - Nicholas Piscitelli
- Property Inventory Manager - Jose Aguilar
- BEST CIO - Mark Raymond
- Local and/or State Police

Introduction

Level 2: PII/PHI Sent or Received in E-mail

Response team may vary.

- PS18-1802 Overall Responsible Party - Heidi Jenkins
- PS18-1802 Data Security Manager - Heather Linardos
- TB/STD Data Security Manager – Linda Ferraro
- 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 HCV work areas are on the first floor which includes many other programs;
- Visitors to the complex must sign in with Security at which point they are photographed and assigned an adhesive visitor's pass;
- Visitors must be escorted while inside the work area;
- DPH security protocol – identification badges (Appendix 6).

Workstations

- Workstations in the HIV Surveillance Program area are outfitted with 65" high panels topped with 14" glass "stack-ons." The workstations also include privacy walls, locking file drawers and locking overhead cabinets;
- Individual staff is personally responsible for safeguarding confidential materials in their workstation;
- Workstation computers must be locked when not in use or unattended (press <ctrl+alt+delete> keys at the same time and select Lock);
- PII/PHI may be kept at individual workstations when needed for surveillance activities. When not in use, PII/PHI must be locked in a desk drawer or filing cabinet;
- 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 the walkway;
- Work areas must be checked at the end of the work day to assure all confidential information has been locked in a desk or cabinet;
- File cabinets and desk drawers containing PII/PHI must be locked when staff are away from their desks;
- Workstation desktop or laptop computers must be shut down or locked.

Off-site Workstations

- Program Coordinators must grant permission for off-site work;
- DIS staff in the STD Program 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 is not present;
- PII/PHI that are no longer needed offsite must be shredded or securely removed to DPH;
- Access to the DPH server from off-site offices must utilize a Virtual Private Network (VPN). The ORP will approve users for VPN access and will assign users to a corresponding token group ID. DPH IT will provide security token devices with built-in authentication mechanisms. Network access must be via McAfee-encrypted devices including tablet, laptop or desktop computer;
- Off-site offices should must have a cross-cut shredder;
- Agency-provided devices must be secured in a locked desk or cabinet when not in use;
- DPH staff may need to share PII/PHI with authorized local staff or others as appropriate to ensure care and follow-up of HIV, STD, TB, HCV or other cases of reportable disease;
- This policy is applicable to any TB, HIV, STD or HCV 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 discussion in 'E-mail').

Telecommuting

- DPH surveillance activities using PII/PHI may be conducted off-site at places of residence or alternative offices by staff approved for telecommuting;
- The Program Coordinator will only approve telecommuting for staff members who have a demonstrated ability to safeguard PII/PHI while off-site;
- Telecommuters:
  - must use DPH-issued electronic devices and secure internet connection to access files or applications on the DPH network for business purposes;
  - will inform their supervisor and Program Coordinator when using PII/PHI off-site;
  - will only use the minimum PII/PHI necessary;
  - will describe how they will protect PII/PHI in their TC application.
- Work will be conducted using DPH-encrypted laptops or other state-owned equipment;
- Internet access must be by using a secure, password protected private connection;
- PII/PHI will not be kept on the TC's personal computer or other personal electronic devices;
- Paper materials or storage media in use at the TC 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 discussion in 'E-mail').

Field Work

- TB, HIV, STD & HCV field work is conducted by epidemiologists reviewing medical records or retrieving data from laboratories, Disease Intervention Specialists (DIS) conducting interviews with STD and HIV cases and TB staff conducting case management activities;
- The appropriate supervisor must always be aware of how PII/PHI are being used in the field;
- Staff must consult with their supervisor before using PII/PHI in new ways;
- Supervisors must periodically review with staff how PII/PHI are secured during working hours and after working hours;
- Loss of PII/PHI or other breaches must be reported to the supervisor as soon as possible;
- Staff must take precautions to minimize risk while traveling to and from external work sites;
- Whenever possible, staff must attempt to accomplish goals without the use of PII/PHI;
- Lists of persons reported with specific reportable diseases must never be taken off-site without supervisory permission;
- PII/PHI must be given to or discussed with non-DPH staff involved in case management only as necessary. Discussions or interviews must be held in private;
- Medical record reviews must be conducted where confidentiality can be assured;
- Any paperwork that is collected or documented from a medical record review must be maintained in a secure setting until returned to DPH;
- The ORP shall issue HIPAA access letter to staff that conduct field work; (Appendix 7)
- DPH staff will carry the DPH HIPAA access letter and present it to facility or laboratory staff to verify authority to access PII/PHI on behalf of DPH. Staff will also carry their DPH photo ID;
- PII/PHI extracted from medical records must be the minimum necessary and limited to that required by the Case Report Form;
- If possible, shred PII/PHI before leaving the facility;
- PII/PHI must not be recorded in calendars, planners, or notes unless indispensable for case management;
- PII/PHI must not be entered into personal devices including laptops (except as discussed elsewhere), mobile devices, cell phones, tablets or other personal electronic devices. Use of a state phone is acceptable but the phone must be password protected;
- PII/PHI must not be left unattended in a vehicle;
- If it is determined that the safest course of action is to leave PII/PHI in a vehicle, it must be kept out of view, preferably locked in a trunk, or under a seat if there is no trunk;
- If PII/PHI needs to be taken to a staff person's residence, PII/PHI must be secured until it can be returned to DPH;
- No one, including family members, should have access to PII/PHI;
- E-mail to and from off-site locations must not include PII/PHI.

Physical Security

Mail

- Program mailboxes are located inside the 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. Mail is then delivered to program staff when available 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 programs are secured from view;
- Laboratories and providers are requested to address mail containing case information to DPH;
- Envelopes 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 locked in a 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

- Once cases can be archived, paper records 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;
- TB, STD and hepatitis C records are 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 controlled by 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;
- The room is windowless and has one entrance;
- Access to the locked room is limited to authorized Surveillance Program staff;
- A master key is in the possession of physical plant staff.

Physical Security

Record Retention

- TB, HIV, STD and HCV paper reports are retained according to the DPH retention schedule (Appendix 8);
- Electronic records are kept indefinitely as part of surveillance registries.

Shredding

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

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 holds an authorized proximity card. No other DPH staff have the same physical access;
- Electronic files, applications and databases reside on the virtual server environment;
- In addition to TB, HIV, STD and HCV, DPH servers contain electronic confidential records of many DPH programs;
- DPH IT staff is 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 Coordinator.

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 9, 10)

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 and VPN to access DPH servers.

Telecommuting

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

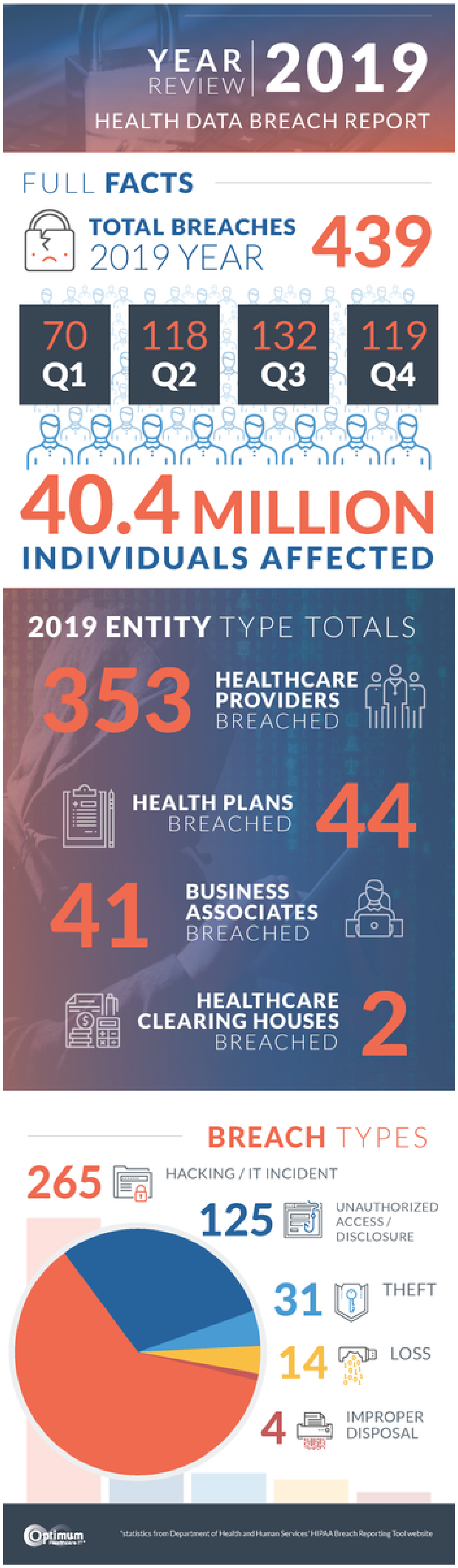
Field Work

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



*statistics from Department of Health and Human Services' HIPAA Breach Reporting Tool website

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 HIPAA Breach Reporting Tool website, the 439 health data breaches reported in 2019 represents 40.4 million potentially affected individuals. (Appendix 11)

Although risk will NEVER BE ZERO, there are ways DPH and BEST help improve the odds of avoiding a data security breach.

✓ 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 BEST 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 WiFi

DPH offers customers and guests separate WiFi access to help protect sensitive data.

Data Security

Devices

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

- Storage devices: (includes but not limited to) USB flash drives, external drives, and SD cards;
- Mobile devices: (includes but are not limited to) laptops, notebooks, IPads, tablets, mobile phones, or any device with photographic/storage capability.

(Appendix 12, 13)

Network

- Electronic files that contain PII/PHI must be stored on the appropriate Program server – not on workstation computers (except when 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 BEST 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 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 .

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 BEST 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

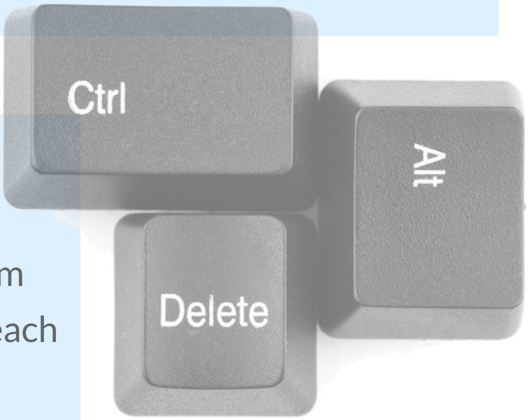
- All workstation computers have access to the internet with 128-bit cipher strength.

Desktop Computers

- A user-ID/password is required to gain access to workstation computers and to the 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 an activated password-protected screensaver.

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 logon screen**
7. Click **OK**
8. The logon will ask you for your usual 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> keys at the same time and select 'Lock.'

Laptop Computers

- All DPH laptops are required to have current DPH encryption software;
- After six months without update, laptops become inaccessible;
- Safeboot: National Institute of Standards and Technology (NIST) certified encryption algorithm, AES FIPS 256 compliant, cannot be bypassed by the user, fully encrypts all files on the hard drive including operating system files;
- Laptop computers are not used for routine surveillance purposes (e.g., case information is not collected directly into laptops, registries are not installed on laptops);
- Use of laptops for case management purposes must be approved by the supervisor and 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 New Haven Health Department 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 .

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;
- Any 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 13, 14)

E-mail

- Any 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 personal 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, PII/PHI must be deleted;
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. **Report the breach: Breach Incident Report**

MailGate

- Assigned staff may use MailGate e-mail as a DPH-approved method for transmitting confidential information;
- This system will be used by STD and TB staff in 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 the needed information.

Telephone Communication

- Telephone communication of PII/PHI is made only to authorized individuals. When in doubt, ask those who are calling to make requests through the mail. Alternatively, 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 using a quiet voice 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 voicemail boxes 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

- There is no such thing as a 'secure' Fax transmission;
- Faxes may be used to send PII/PHI to laboratories or medical providers when rapid communication is necessary;
- Disease-specific references (HIV, AIDS, CD4, Syphilis, Hepatitis C, etc., or related terminology) must be avoided in the content and fax cover. The fax header must also not include these references;
- 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 15);
- 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 UBS Drives

- USB drives used to transport PII or PHI must be cleared after use;
- EaseUs Partition Master 13.5 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 can use a secure FTP connection to upload or download files;
- Immediate supervisor will determine DPH-user server or client role in the data transfer protocol;
- Notify the DSM when sFTP account is activated;
- Files should be encrypted prior to posting in the client/server architecture;
- Passphrase or public keys must 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 the ct.gov site;
    - The CDC administered Public Health Information Network (PHIN-MS);
    - DAS/BEST managed B2B VPN connections between corporate end points (most appropriate for hospital or Connecticut-based laboratory installations);
    - Token based VPN authentication managed through DAS/BEST 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 the State Mobile Device Policy (Appendix 12);
- 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 and after approval referred to the appropriate Data Manager;
- Data subsets (data sets) from the registry used for analysis must include 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 Surveillance Program server domains;
- 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-mails;
- Analysis products must be approved by the appropriate Program Coordinator before being sent to the data customer to confirm results, do not contain inappropriately small cell sizes, and do not contain sensitive information.

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;
- Proposed analyses where the numerator or denominator is small, 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 Hawaiian or Alaska Natives;
    - 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 completed and ready to be sent to the customer (including to CDC), Data Managers must confer with the appropriate Program Coordinator to ensure that potentially identifying information is not disclosed;
- CDC release of Connecticut data will conform to the current data release agreement between 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 (see data suppression section, above);
- 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.

Sharing PII/PHI

- PII/PHI are not released except in situations where public health need is compelling, control over confidentiality assured, and where it is not specifically prohibited by statute;
- Permission of the Program Coordinator is always needed to release PII/PHI. ORP permission is sometimes needed;
- Only the minimum necessary PII/PHI is released;
- Data that is transmitted to other programs or outside agencies by electronic file (or other transport medium) must be encrypted;
- Sharing of PII/PHI are permissible only under the following circumstances:

Local Health Departments (LHD)

- HIV: HIV is not reportable to LHD. However, an option exists for LHD to receive HIV surveillance data for public health purposes (referral to care, partner notification). 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 16) (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 Hepatitis C Prevention Program may communicate information to LHD, as needed, for implementation of local control measures.

Inter-state HIV Surveillance Programs

- Designated staff in HIV Surveillance programs in other states may be contacted to complete case information and establish residency and case “ownership.”

National Death Index

- National Death Index data is used to match with the HIV Surveillance Registry to determine vital status. In this CDC-designed protocol, encrypted HIV data are shipped to the National Center for Health Statistics for matching;
- Potential matches are reported back to DPH for evaluation.

LexisNexis

- LexisNexis is used to ascertain additional information about reported cases including address, alias names, vital status, and contact information;
- Only designated staff members conduct these 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;
- If external, approval from the external IRB/HIC may also be required;
- Appropriate Program Coordinator and ORP approval is required;
- Consent of the cases or subjects may be required;
- In cases of research that does not involve PII/PHI, the Program Coordinator will consult with the IRB/HIC Chair to determine if IRB/HIC approval is needed.

Data Sharing within DPH

- Information about reportable conditions can be exchanged freely between programs authorized to conduct surveillance for those conditions.

eHARS Access (CDC - National HIV/AIDS Reporting System)

- Multiple TB, HIV, STD and HCV Section staff are allowed read-only access to eHARS for case investigation purposes;
- Staff must review this policy and sign a Confidentiality Agreement prior to access being granted;
- Staff with access to eHARS are trained to navigate the system by HIV Surveillance Program staff.

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 and using DPH-provided software. A variety of matching programs are available for use;
- Files used in matching are encrypted or deleted when not in use;
- Matching is periodically conducted between HIV and Vital Records to ascertain perinatal exposure cases and update vital status;
- Hepatitis C matching with HIV occurs approximately annually to characterize co-infected cases;
- STD matching periodically occurs to characterize individuals who are co-infected;
- TB matching with HIV is done to identify HIV positive cases and change case status from HIV to AIDS for HIV cases with TB.

Other Sharing Requests

- DPH data sharing policy allows for any DPH Program 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;
- Programs within Infectious Diseases are administratively combined and do not need to use the data sharing form.

Routine Surveillance Data Reporting

- Routine HIV surveillance data are reported monthly using CDC Secure Access Management Services (SAMS);
- Routine STD, TB and hepatitis C data are reported to CDC using National Electronic Disease Surveillance System (NEDSS).

Program Severance

- Section staff who retire, are terminated, resign from DPH, or change jobs within DPH (outside of the Section) are no longer authorized to access or utilize PII/PHI contained in any data system within the TB, HIV, STD, and/or HCV Programs;
- The DPH Help Desk must be contacted to revoke access to secure drives, the sFTP and to wipe VPN drive mapping;
- Program Coordinators must revoke access to ancillary data bases and systems;
- 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 person's last day.

(Appendix 17)

Data Security Recap

Desktop Computers

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

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

Data Sharing

DPH data sharing policy allows for any DPH Program to request data from other Programs for public health use

Confidentiality Agreement

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

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

(Appendix 18)

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

Click here to complete the Confidentiality Agreement or go to this link: https://www.surveymonkey.com/r/DPH-Confidentiality-Agreement

Thank you!