Confidentiality Guidelines for HIV/STD/TB/Hepatitis Surveillance Programs 2017

Contacts:

Rory Angulo, MD, MBA (STD, HIV)
(860) 509-7900
rory.angulo@ct.gov

Heidi Jenkins (STD, TB, HIV, Hepatitis)
(860) 509-7920
heidi.jenkins@ct.gov

410 Capitol Avenue
PO Box 340308
Hartford CT 06134-0308

Last revision December 22, 2016
# Table of Contents

## Introduction

- Public health surveillance data
- Confidential information
- Confidentiality guidelines
- Confidentiality agreement
- Overall responsible person (ORP)
- Breach of confidentiality
- Personally identifying information

## Physical security

- Building
- Paper record storage
- Workstations
- HIV locked room
- Offsite workstations
- Record retention
- Telecommuting
- Shredding
- Field work
- Physical security of servers
- Mail
- Disaster Recovery Plan

## Data security

- Network
- Printing
- Server backup
- Electronic lab reporting
- Internet
- Data entry
- Computers
- Data dissemination
- Laptop computers
- Routine data requests
- Use of smart phones/tablets
- Data suppression
- E-mail
- Analysis using GIS
- Telephone communication
- Release of PII/PHI
- Fax communication
- Routine reporting to CDC
- Retirement of hard drives

## Appendices

1. Reportable Diseases and Laboratory Findings (Reg.19a-36) ............................................. 15
2. Disclosure of Health Data (Reg.19a-25) .............................................................................. 20
3. Federal Assurance of Confidentiality .................................................................................. 23
4. Confidentiality Agreement ................................................................................................... 24
5. DPH Security Protocol – identification badges ................................................................. 25
6. HIPAA Access Letter .......................................................................................................... 26
7. Retention Schedule ............................................................................................................ 27
8. Fax Disclaimer ..................................................................................................................... 31
9. PCSI Disaster Recovery Plan ............................................................................................. 36
Introduction

Public health surveillance data:
- HIV/STD/TB/Hepatitis surveillance data are collected in accordance with Connecticut regulation 19a-36 (Appendix 1).
- Data are collected for public health purposes only.
- The minimum data are collected that satisfy public health surveillance needs.
- Information is collected, stored, and disseminated in accordance with applicable state regulation and the Federal Assurance of Confidentiality (Appendix 2, 3).

Confidentiality guidelines:
- **DPH Confidentiality Guidelines** describe the policies and methods used to safeguard the confidentiality of surveillance information.
- **DPH Confidentiality Guidelines** are reviewed and updated annually or as needed by the PCSI Coordinator in response to changing technologies, personnel, or policies.
- **DPH Confidentiality Guidelines** cover CDC-funded activities of the HIV/STD/TB/Hepatitis Surveillance Programs. Program-specific guidelines will be labeled (e.g., HIV is not reportable to local health departments). Guidelines that are not specifically labeled apply to all three program areas.
- The DPH guidelines are 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; Atlanta, GA; 2011.

- These guidelines must be considered a minimum standard. There may be scenarios not covered by these guidelines where staff, supervisors and 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 training in confidentiality conducted by appropriate staff as determined by the ORP.
  - Distribution list
    - The **DPH Confidentiality Guidelines** are distributed annually to the following personnel to facilitate training of all appropriate staff.
      - Heidi Jenkins – ORP
      - Rory Angulo – Confidentiality Manager
      - Heather Linardos – HIV Surveillance Program
      - Marianne Buchelli – HIV Prevention Program
      - Laura Aponte – HIV Care and Support Services Program
      - Dr. Lynn Sosa – STD/TB Programs
      - Devon Eddy – Infectious Diseases
      - Eva Golebiewski – IT
Overall responsible person (ORP):

- The ORP must certify annually that DPH is in compliance with CDC guidelines.
- ORP – Heidi Jenkins, Public Health Section Chief, Hepatitis, HIV, STD and TB Section.

Personally identifying information (PII/Protected health information (PHI))

- PII/PHI are defined as any information about an individual, used singly or in combination, including 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 any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Potentially linkable ID numbers in surveillance registries are also considered PII/PHI (HIV state number, medical record number, DOC number).
- Cross-tabulations of case characteristics and rates, if sufficiently specific and if numbers are small, may also be considered PII/PHI.

Confidential information:

- Any information about an identifiable person or establishment, when the person or establishment providing the data or described in it has not given consent to make that information public and was assured confidentiality when the information was provided.

Confidentiality agreement:

- All new DPH employees sign a confidentiality agreement as part of their orientation.
- DPH employees who need access to HIV/STD/TB/Hepatitis PII/PHI must be familiar with the DPH’ HIV/STD/TB and Hepatitis Confidentiality Guidelines and sign a specific Confidentiality Agreement prior to being given access to PII/PHI (Appendix 4).
- By signing the HIV/STD/TB/Hepatitis Confidentiality Agreement staff members agree to abide by the DPH Confidentiality Guidelines and Connecticut Statute 19a-25.
- Annually, appropriate DPH IT staff members sign the Confidentiality Agreement.
- Confidentiality Agreements signed annually are a record of the annual training and kept by the HIV Surveillance Program Confidentiality Manager.
- The Confidentiality Manager maintains a log of DPH staff with access to PCSI confidential information. The log includes date of S&C training and signed CA document.

Breach of confidentiality:

- A breach is defined as an infraction or violation of a standard, obligation, or law.
- Breach in data security – any unauthorized use of PII/PHI.
- Breach of protocol – any violation of the confidentiality guidelines.
- Breach of confidentiality – any unauthorized disclosure of PII/PHI.
- Breaches will be investigated and documented in the breach log, which will be maintained by the Confidentiality Manager.
- Staff should report any known or suspected breaches to the supervisor, Program Coordinator and Confidentiality Manager. Reporting staff must provide the following information when reporting a breach:
  - Date of breach occurrence
  - Breach origin, include names of person causing breach and organization
  - Description of the occurrence.
  - Actions staff has taken to mitigate further impact.
- PCSI Coordinator and Confidentiality Manager will evaluate incidents resulting in the disclosure of confidential information that merit CDC notification.
- The ORP will contact the Connecticut Attorney General’s Office as needed to determine if legal action is needed in consequence of a breach.

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 HIV/STD/TB/Hepatitis work area is the first floor and also includes many other programs.
- Visitors to the complex must sign in with security and be escorted while inside the work area.
- DPH security protocol – identification badges (Appendix 5).

**Workstations:**
- Individual staff is personally responsible for safeguarding confidential materials in their workstation cubicle and for safeguarding access to the DPH network via their computer.
- Program workstations are located in a large open area of cubicles with the possibility of visitors who are non-Program staff and members of the public.
- Workstation computers must be locked when not in use or unattended (“screen lock”, “logout”, or “lock down” computer) (press the <Ctrl+Alt+Delete> keys at the same time, at Windows Security select ‘Lock Computer’).
- PII/PHI may be kept at individual workstations when needed for surveillance activities. When not in use, PII/PHI must be locked in the desk or in filing cabinets.
- Staff must take precautions to ensure that PII/PHI are not in view of unauthorized people.
- All monitors should have a security screen on workstation computer monitors. If possible, monitors should not be visible from the hallway.
- All 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.
- Cabinets/desk must be locked and computers turned off overnight.
**Offsite workstations:**

- Working in an offsite workstation, such as at a local health department, must only be undertaken with the knowledge and permission of the supervisor and Program Coordinator.
- DIS staff in the STD program is assigned work spaces in local health departments.
- Staff must be mindful that offsite workstations may be accessed by non-DPH staff or others in their absence.
- Requirements for security 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 removed to DPH.
- Access to the DPH server from offsite offices must utilize a Virtual Private Network (VPN) connection. The PCSI Coordinator or ORP will approve users for VPN access and will assign users to a corresponding token group ID. DPH IT will provide free-on-board security token devices or VPN key FOB or VPN token with built-in authentication mechanisms. Network access must be by using a DPH safeboot encrypted device, including tablet, laptop or desktop computer.
- The offsite office should include a personal 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 the care and follow-up of STD, TB, or other cases of reportable disease.
- These guidelines are applicable to any HIV/STD/TB/Hepatitis staff located at any offsite workstation either permanently or for temporary projects.
- Email to and from offsite workstations must not include PII/PHI (see discussion in ‘Email’).
- In offsite workstations, staff must be aware that Fax machines, copiers and printers may have hard drives that retain images of materials processed in those devices.

**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 responsible staff members who have a demonstrated ability to safeguard PII/PHI. Telecommuters (TC) are responsible for the appropriate handling of PII/PHI while offsite.
- TC must not use non-state owned electronic devices, nor use a public internet connection for access to files/applications to state network for business purposes.
- TC will inform their supervisor and Program Coordinator when using PII/PHI offsite.
- TC will only use PII/PHI when necessary.
- TC will use the minimum PII/PHI necessary.
- TC will describe in their TC application how they will protect PII/PHI.
- Work will be conducted using DPH encrypted laptops or other state-owned equipment.
- Internet access must be by using a secure/restricted private connection, WPA/encrypted. PII/PHI will not be kept on the TC personal computer or other personal electronic devices.
Connecticut Department of Public Health – HIV/STD/TB/Hepatitis Surveillance Programs - Confidentiality Guidelines

- Paper materials and storage media in use at the TC residence will preferably be kept in locked cabinets but otherwise in a secure location overnight and removed back to DPH when no longer needed or when the telecommuter is on vacation. Locked cabinets or other secure locations will not be shared with or accessible to other household members.
- Other members of the household will have no access to PII/PHI.
- Backup storage media will be secured at DPH.
- Email to and from TC workplaces must not include PII/PHI (see discussion in ‘Email’).

Field work:
- Field work in the HIV/STD/TB/Hepatitis Surveillance Programs 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 the purposes for which PII/PHI are used and how they are secured during the day, during non-work times of the workday, and during non-work hours.
- Loss of PII/PHI or other breach must always be reported to the immediate supervisor.
- With travel to and from external sites there is an increased risk of a breach of confidentiality and staff must take precautions to minimize risk.
- Accomplish goals without the use of PII/PHI (names) whenever possible (initials and DOB).
- Lists of persons reported with specific reportable diseases must never be taken offsite 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 confidential setting until returning to the workstation.
- PCSI coordinator shall issue HIPAA access letter to staff that conduct field work. DPH staff will carry the DPH HIPAA access letter (Appendix 6) 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. (The PCSI Coordinator is working with upper management to determine who the letter should be from and obtain a signature for appropriate use as needed in the future.)
- 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 laptops (except as discussed elsewhere), personal mobile devices, cell phones, tablets or other personal electronic devices. Use of a state phone is acceptable but the phone must be password protected.
• Ideally, 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 but under a seat or in a bag or container if there is no trunk.

• If PII/PHI need to be taken to a staff person’s residence, PII/PHI must be secured until they can be returned to the office. No one, including family members, should have access to PII/PHI.

• Email to and from off-site locations must not include PII/PHI.

**Mail:**

• Mailboxes are located inside the work area. Mail is received in US Mail or interoffice envelopes. Typically, mail is delivered at 11:00AM.

• Clerical staff is tasked with twice a day mail pickup. HIV mail is then delivered to program staff when available or stored in a specific drawer in an assigned locked cabinet. Keys to the cabinet are always kept in the Surveillance Program.

• Mail must be collected promptly on delivery and checked again at the end of the day.

• Mailboxes within individual programs are secure from viewing by those who are not staff from these programs.

• Laboratories and providers are requested to address mail containing case information to:
  
  Connecticut Department of Public Health  
  410 Capitol Ave (mail-stop code)  
  PO Box 340308  
  Hartford CT 06134-0308  
  Envelopes marked “CONFIDENTIAL.”

• When reports are inadvertently mailed to the wrong Program, mail must be locked in a cabinet/desk if it cannot be forwarded immediately. Mail must be forwarded in sealed interoffice envelopes to the appropriate Program. Opened mail must not be left unattended in cubicles. On an annual basis, all administrative staff in the Infectious Disease Division receives and discusses the Confidentiality Guidelines, and signs a Confidentiality Agreement.

• Mail, both from outside sources and in interoffice envelopes, that is 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. This is either lockable filing cabinets or in boxes in a designated locked room.

• Ultra-long term storage of paper TB records (10 years at DPH and 11–60 years offsite). Off-site storage is at a state-owned facility in Rocky Hill. The site has been visited by DPH staff but staff members at the facility are responsible for security and confidentiality.

• TB/STD/Hepatitis records are stored in the DPH long-term storage area in a locked room.

• Access to DPH locked rooms is limited to appropriate surveillance 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 PCSI Program staff. A master key is in the possession of physical plant staff.

**Record retention:**
- HIV/STD/TB/Hepatitis paper reports are retained according to the DPH retention schedule (Appendix 7).
- 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. As these personal shredders wear out they will be replaced with crosscutting shredders.
- There are three crosscutting shredder available to staff. They are located in the following program areas: HIV Surveillance, HIV Prevention and TB.
- Annual shredding is conducted using an agency-approved vendor shredding service. The shredding vendor (Infoshred) is used periodically to shred STD and TB paper. The Infoshred truck comes to the site, staff must observe shredding, and shredded material is re-shredded to dust when the truck returns to its home office. An assigned HIV Surveillance staff person observes the shredding process when shredding of HIV documents occurs.

**Physical security of the servers:**
- DPH servers are located in one physical location at the 410 Capitol Avenue building.
- Access to the IT work area floor is by way of proximity cards.
- Servers are inside a secure room, with only one door. Access to the room is restricted exclusively to staff that holds an authorized proximity card. No other DPH staff with a proximity card has the same level of physical access.
- Electronic files, applications and databases reside on the virtual server environment.
- In addition to HIV, STD, TB and Hepatitis, DPH servers contain the 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 appropriate Surveillance Coordinator.

**Disaster Recovery Plan**
- Instances that require restoration of PCSI program files, applications or databases are evaluated by the PCSI Coordinator and/or Confidentiality Manager prior to declaration of disaster.
• The PCSI team lead, as noted on the PCSI DRP document, will activate the DRP plan and coordinate with the DPH IT team for the restoration of hardware/software as required to attain normal PCSI activities.

• PCSI staff will follow the actions required as set forth in the DPH IT DRP document, or as assigned, when the lead team requires of his/her assistance.

• The DRP document must be maintained and updated after DR exercise reports to address gap issues and as new technology takes place.

• The DRP document must be maintained by the PCSI Coordinator/Confidentiality Manager to reflect changes in team contact information, vendors or other critical information.

• PCSI staff can have access to the DRP document, which can be found on the shared directory drive at the following location: ‘U:\SHAREDOC\PCSI_docs_gen’.

• The DRP is under Appendix 9.

Data security

For purposes of data security, the following are defined as:

• Storage devices – including but not limited to CD/DVD, USB memory drives, external drives, any devices capable of storing data such as regular/micro SD cards, memory sticks, zip disks, etc.

• Portable devices – including but not limited to laptops, notebooks, Ipads, tablets, cell phones, any device with photographic/storage capability

Network:

• Electronic files that contain PII/PHI must be stored on the appropriate Surveillance Program server – not on workstation computers (except when noted in this document).

• The DPH IT network administrator, with approval of the PCSI Coordinator, 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 confidentiality training and sign the Confidentiality Agreement.

• The DPH network, servers, and computers are protected by McAfee virus software ISS (IBM Proventia Site Protection).

• 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 Nick Piscitelli.

• DPH IT continually upgrades the data security environment in response to evolving technology and potential security threats.

Server backup:

• An encrypted tape backup copy of DPH server content is made daily and stored in IT. Weekly, a backup tape is sent off-site to a private company.
• Backups of all DPH and BEST servers run nightly.
• Servers are backed up to an attached Dell PowerVault TL4000.
• Data is encrypted using 256bit AES (Advanced Encryption Standard) scheme before being added to the tape.
• Off-site storage: MEYER | Records Management, Windsor, CT
• Recovery of information from backup tapes is not possible without highly specialized software, equipment, and skills.
• Use of backup copies to restore files is requested through the appropriate Surveillance Coordinator and network administrator.
• When data file(s) /directory/application restoring is required, the PCSI Coordinator/Confidentiality Manager will follow procedures as described in the ‘Server Data Backup Procedures’ document, which is maintained by DPH IT. A copy of the document can be found at ‘X:\procedures manual’.

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

Computers:
• A user-ID/password is required to gain access to workstation computers and to the network.
• Password changes are required every 30 days.
• CT DPH is taking measures to comply with the Federal Social Security Administration of the Active Directory password policy by implementing a new password standard (01/27/2015).
• Workstation computers must have an activated password protected screensaver.
  o Creating a screen saver password
    1. Click on the Windows icon in the banner on the lower left corner of your display
    2. Click on “Control panel”
    3. Click on “Appearance and Personalization”
    4. Under “Personalization” click on “Change Screensaver”
    5. Choose a screensaver, choose a time after which it will come on, and check the box “On resume display login screen”
    6. Click OK
    7. The login will ask you for your usual password. You don’t need a new password for this.
• 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 (“screen lock”, “logout”, or “lock down” computer (press the <Ctrl+Alt+Delete> keys at the same time, at Windows Security select ‘Lock Computer’).

Laptop computers:
• All DPH laptops are required to have DPH encryption software and be periodically updated. After six months without an update laptops become inaccessible.
• Safeboot: NIST certified encryption algorithm; AES FIPS 256 compliant; cannot be bypassed by the user; fully encrypts all files on 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.
• MHS staff uses an encrypted laptop to transport data from the laboratory to DPH.
• With approval of the appropriate Program Coordinator and for the duration of a non-routine surveillance activity, DPH laptops that have been encrypted by DPH IT staff may be used.
• Telecommuters are authorized to use encrypted DPH laptops.
• Staff may use encrypted DPH laptops at authorized offsite workstations.

**Use of storage or portable 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 (version 1.0, issued 09/10/2007)
• 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.
• Thumb drives or other standalone 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. These devices must be in locked drawers when not in use. These devices must not be left unattended in a vehicle.

**Electronic mail:**
• Staff must be aware that email can become publicly available under the Freedom of Information Act.
• Work email is not private and copies reside in administrative servers and backup systems.
• Except as described below, email to DPH staff or to addressees outside DPH is not used to transmit PII/PHI or attached files (including encrypted files) containing PII/PHI. This applies to use of the DPH email system from inside DPH or external use via internet access of DPH email.
• Email must include an automatic signature block stating that email must not be used to transmit PII/PHI. To setup automatic signature in MS Outlook click on ‘File’\’Options’\Mail’\Signatures…’ toggle. Template: ‘Please **do not respond to this email with any patient identifying information (PII)**. 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, please contact me at my confidential phone line. Thank you.
• If email is received which includes PII/PHI, the following steps must be taken: delete the email containing the PII/PHI, if responding to the email, PII/PHI must be deleted, remind the sender not to send PII/PHI through email as DPH email is not secure or encrypted and ask that the email with the PII be deleted from all email folders (including sent and deleted folders).
• Assigned staff may use MailGate email as a DPH-approved method for transmitting confidential information. This system will be used by STD and TB staff in communicating with healthcare 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 email systems initiated by another person sending an email to the DPH staff member from outside of the state email 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 email systems, PII/PHI should be kept to the minimum necessary to communicate the needed information.

**Telephone/cell phone communication:**

• Telephone communication of PII/PHI is made only to known, authorized individuals.

• When in doubt, make requests and 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 other states conducting surveillance. CT DPH PCSI programs can obtain a copy of the posting from CDC’s portal (Sitescape, SAMS, Sharepoint, etc.) 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 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 any PII/PHI information. All text communications must 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 but only when rapid communication is highly desirable and disease-specific references (HIV, AIDS, CD4, Syphilis, Hepatitis B, etc., or related terminology) must be avoided whenever possible in the content or Fax cover. The Fax header must also not include these references.

• The sender should ensure that the Fax number is correctly entered and try to contact the person receiving the Fax by phone prior to sending to request that the Fax is retrieved immediately.

• Whenever practical, lists that need to be sent to laboratories or medical records departments must be sent by registered US Mail or by commercial courier. This will take more time and additional planning may be needed.

• The Fax cover page must include a disclaimer (Appendix 8).
Fax users must notify the appropriate supervisor and investigate misdialed Faxes to secure confidential information.

The Fax machine must be checked each night to ensure that PII/PHI are not in the in-tray.

**Retirement of hard drives:**
- Computer, laptop and server hard drives scheduled for retirement are separated from the computer chassis and degaussed, and then surplused as scrap.
- When an older copier or Fax machine is retired a vendor technician will remove the drive and turn it over to IT to be destroyed or erased.
- The Document Center hard drives are encrypted.

**Printing:**
- Only with prior approval from the supervisor and Program Coordinator should lists of cases be printed. This includes comprehensive lists of cases for specific facilities or other lists.
- Confidential print jobs must be sent to a printer within a Program cubicle if one is available. 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 data with non-DPH agencies will use a secure ftp connection to post/download files.
- Immediate supervisor will determine DPH-user server or client role in the data transfer protocol.
- Notify S&C manager when sftp account is activated.
- As possible, files should be encrypted prior to its posting in the client/server architecture.
- Passphrase or public keys must be exchanged via email or by a phone call.

**Electronic laboratory reporting (ELR):**
- ELR is a system being developed by DPH for electronically reporting laboratory findings directly by laboratories to DPH. This section of the Confidentiality Guidelines will be updated as the system reaches full ELR implementation to reflect interim security and confidentiality measures that may be needed.
- Currently, electronic file transmission of laboratory reports of significant findings is achieved by the following file reporting format and transport mechanisms:
  - Electronic files, any file format (HL7, .csv., .txt, .dat, etc) that are not using ELR/PHIN MS instance must be encrypted using PGP. Recipient DPH staff must provide a PGP public key to the reporting party. The reporting party will associate the file with recipient’s public key during the file encryption process.
  - The reporting party will post the encrypted file to CT DPH sftp site, or to the lab’s secure site, or to the lab’s third party vendor that manages their secure file exchange.
  - Alternatively, reporting parties not able to use an electronic delivery method have the option to encrypt or password-protect the file and burn it on a CD. Mailing of CDs
must follow directives described in the ‘Mail’ section of this document. A password will be provided to the recipient using a different method (e-mail or phone call).

- Laboratories within CT that perform HIV genotype testing and have the equipment analyzer on-site that is not networked or unable to export results can request assistance from DPH for data extraction. DPH staff must use a USB FIPS 140-2 compliant drive or an encrypted laptop as the final location during the file transfer prior to leaving the building where the file is extracted from. Upon arrival to the agency, DPH staff must relocate the file to a secure location within the agency network. DPH staff must take the files from laptops and recycle bins and format a USB drive utilized during this task.

**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 up any PII/PHI when leaving their cubicle.

**Data dissemination:**
- Standard tables and graphs are released annually on the DPH webpage.
- 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 or designee.
- Data subsets (datasets) from the registry used for analysis must include the minimum elements necessary and must not include PII/PHI unless necessary.
  - Encrypt or delete datasets when not in use. Pretty Good Privacy (PGP) is an encryption program that supports cryptographic privacy and authentication for data communication. PGP is the DPH standard.
  - Store datasets in assigned Surveillance Program server domains.
  - Never put datasets on workstation computers, laptops, thumb drives, or in unauthorized server domains.
  - Never attach datasets to emails.
- Analysis products must be approved by the appropriate Program Coordinator before being sent to the data customer to confirm that they answer the question being asked, do not contain inappropriately small cell sizes, and do not otherwise contain sensitive information.

**Data suppression (low cell size and numerator/denominator rules):**
- 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 Native.
  - Transgender or other infrequent gender categories.
  - Small or single-year age groups.
  - Infrequent risk behavior categories (e.g., perinatal, needle stick).
  - 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).

**Analysis using GIS:**

- If PII/PHI will be 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.

- Datasets being used for GIS analysis must be kept in the appropriate 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, as noted below.

- Only the minimum necessary PII/PHI is released.
• Data that is transmitted to other programs or outside agencies by electronic file (CD or other transport medium) must be encrypted. PGP is the DPH standard.
• Sharing of PII/PHI are permissible only under the following circumstances:
  o 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 take advantage of this option, 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. https://www.cdc.gov/rdc/Data/b4/section308.pdf
    ▪ **STD**: 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. The TB Program may communicate case information to LHD, as needed, for implementation of local control measures.
    ▪ **Hepatitis**: Hepatitis B and C is reportable to LHD. The Hepatitis Program may communicate information to LHD, as needed, for implementation of local control measures.
  o Surveillance programs in other states may be contacted to complete case information and establish residency and case ownership.
  o National Death Index has been used to match HIV cases 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.
  o Lexis Nexis 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.
  o Research involving PII/PHI where Institutional Review Board (IRB) approval has been obtained. Research may be internal to DPH or external. If external, approval from the external IRB may also be required. Appropriate Program Coordinator and ORP approval is also required. Consent of the case may also be required. In cases of research that does not involve PII/PHI, the Program Coordinator will consult with the IRB Chair to determine if IRB approval is needed.

  o Data sharing within DPH
    ▪ Information about reportable conditions can be exchanged freely between programs authorized to conduct surveillance for those conditions.
    ▪ **STD Program**: A designated STD staff member routinely accesses eHARS to determine the HIV status of newly reported STD cases.
    ▪ 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 PCSI program.
✓ Matching must be conducted by a PCSI staff, within DPH and using DPH-provided hardware. A variety of matching software 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 B/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 reporting of surveillance data to CDC:**
- Routine HIV surveillance data (Core, GIS, Incidence and MHS) are reported using SAMS.
- Routine STD, TB and Hepatitis data are reported to CDC using NETSS.
Appendix 1:

Reportable Diseases and Laboratory Findings

19a-36-A1. Definitions
As used in Sections 19a-36-A1 to 19a-36-A56:

(a) "Authorized agent" means an individual designated by a local director of health to act for him or her in the performance of any of his or her duties.

(b) "Carrier" means an infected person or animal who, without any apparent symptoms of communicable disease, harbors a specific infectious agent and may serve as a source of infection for humans. The state of harboring a specific infectious agent may occur in an individual with an infection that is inapparent throughout its course (asymptomatic carrier), or in an individual during the incubation period, convalescence, and post-convalescence of a clinically recognizable disease (incubatory carrier and convalescent carrier). The carrier state may be of short duration (transient carrier) or long duration (chronic carrier).

(c) "Case" means a person or animal who exhibits evidence of disease.

(d) "Cleaning" means the process of removal of organic matter conducive to growth or maintenance of infectivity of infectious agents by scrubbing and washing as with hot water and soap.

(e) "Commissioner" means the state commissioner of health services.

(f) "Communicable disease" means a disease or condition, the infectious agent of which may pass or be carried directly or indirectly, from the body of one person or animal to the body of another person or animal.

(g) "Communicable period" means any time period during which a specific infectious agent may be transferred directly or indirectly from an infected person or animal to another human or animal.

(h) "Contact" means a person or animal known to have had association with an infected person or animal in such a manner as to have been exposed to a particular communicable disease.

(i) "Contamination" means the presence of undesirable substance or material which may contain an infectious agent on external body surfaces (e.g., skin), articles of apparel, inanimate surfaces or in food or beverages.

(j) "Cultures" mean growths of an infectious agent propagated on selected living or artificial media.

(k) "Date of onset" means the day, month and year on which the case or suspected case experienced the first sign or symptoms of the disease.

(l) "Department" means the Connecticut Department of Health Services.

(a) "Disinfection" means a directly applied chemical or physical process by which the disease producing powers of infectious agents are destroyed.

(1) "Concurrent disinfection" means the immediate disinfection and disposal of body discharges, and the immediate disinfection or destruction of all infected or presumably infected materials.

(2) "Terminal disinfection" means the process of rendering the personal clothing and immediate physical environment of a patient free from the probability of conveying an infectious agent to others after removal of the patient or at a time when the patient is no longer a source of infection.

(n) "Epidemic" means the occurrence of cases of illness clearly in excess of normal expectancy over a specific time period in a community, geographic region, building or institution. The number of cases indicating an epidemic may vary according to the causative agent, size and type of population exposed, previous experience with the disease, and time and place of occurrence. An outbreak of disease is an epidemic.

(o) "Epidemiologic investigation" means an inquiry into the incidence, distribution and source of disease to determine its cause, means of prevention, and efficacy of control measures.

(p) "Foodborne outbreaks" means illness in two or more individuals acquired through the ingestion of common-source food or water contaminated with chemicals, infectious agents or their toxic products. Foodborne outbreaks include, but are not limited to, illness due to heavy metal
intoxications, staphylococcal food poisoning, botulism, salmonellosis, shigellosis, Clostridium perfringens intoxication and hepatitis A.

(q) "Foodhandler" means a person who prepares, processes, or otherwise handles food or beverages for people other than members of his or her immediate household.

(r) "Health care facility" means any hospital, long term care facility, home health care agency, clinic or other institution licensed under Chapter 368v of the Connecticut General Statutes and also facilities operated and maintained by any state agency for the care or treatment of mentally ill persons or persons with mental retardation or substance abuse problems.

(s) "Health care provider" means a person who has direct or supervisory responsibility for the delivery of health care or medical services. This shall include but not be limited to: licensed physicians, nurse practitioners, physician assistants, nurses, dentists, medical examiners, and administrators, superintendents and managers of health care facilities.

(t) "Incubation period" means the time interval between exposure to a disease organism and the appearance of the first symptoms of the resulting disease.

(u) "Infection" means the entry and multiplication of an infectious agent in the body of a person or animal with or without clinical symptoms.

(v) "Infectious agent" means a microorganism capable of producing infection with or without disease.

(w) "Isolation" means the use of special precautions during the period of communicability to prevent transmission of an infectious agent. Such special precautions may include: physical separation of infected persons or animals from others, or precautions such as blood precautions that do not necessarily result in physical separation of individuals.

(x) "Laboratory" means any facility licensed, or approved by the department in accordance with section 19a-30 of the Connecticut General Statutes.

(y) "Local director of health" means and includes the city, town, borough or district director of health and any person legally authorized to act for the local director of health.

(z) Medical information" means the recorded health information on an individual who has a reportable disease or who has symptoms of illness in the setting of an outbreak. This information includes details of a medical history, physical examination, any laboratory test, diagnosis, treatment, outcome and the description and sources of suspected causative agents for such disease or illness.

(aa) Nosocomial infection" means infections that develop within a hospital or other health care facility or are produced by microorganisms acquired while in a hospital or health care facility.

(bb) Outbreak." See "epidemic."

(cc) Quarantine" means the formal limitation of freedom of movement of persons or animals exposed to, or suffering from a reportable disease for a period of time not longer than either the longest incubation period or the longest communicable period of the disease, in order to prevent spread of the infectious agent of that disease.

(dd) Reportable disease" means a communicable disease, disease outbreak, or other condition of public health significance required to be reported to the department and local health directors.

(ee) Reportable laboratory finding" means a laboratory result suggesting the presence of a communicable disease or other condition of public health significance required to be reported to the department and local health directors.

(ff) State epidemiologist" means the person designated by the Commissioner as the person in charge of communicable disease control for the state.

(gg) Surveillance" means the continuing scrutiny of all aspects of occurrence and spread of a disease relating to effective control of that disease, which may include but not be limited to the collection and evaluation of: morbidity and mortality reports; laboratory reports of significant findings; special reports of field investigations of epidemics and individual cases; data concerning the availability, use, and untoward side effects of the substances used in disease control, such as rabies vaccine; and information regarding immunity levels in segments of the population.

(hh) Suspected case" means a person or animal suspected of having a particular disease in the temporary or permanent absence of definitive clinical or laboratory evidence.

(ii) Other condition of public health significance" means a noncommunicable disease caused by a common source or prevalent exposure such as pesticide poisoning, silicosis or lead poisoning.

Effective October 25, 1989.)

Effective October 25, 1989.)
19a-36-A2. List of reportable diseases and laboratory findings
The commissioner shall issue a list of reportable diseases and laboratory findings within sixty days of the effective date of these regulations, on the next January 1, and annually thereafter. The list shall show it is the current list and shall specify its effective date. This list shall also include but not be limited to the reporting category of each disease, procedures for the reporting, and minimum investigation and control measures for each disease. Listed diseases are declared reportable diseases as of the effective date of approval by the commissioner.
(a) The commissioner in consultation with the state epidemiologist will annually review the existing list and develop recommendations for deletions or additions to the list.
(b) The state epidemiologist or other commissioner designee shall convene and chair an advisory committee to review the recommendations for any changes to the list prior to preparing the final list for that year. This committee shall make recommendations to the commissioner regarding the contents of the list.
(c) The commissioner shall review the advisory committee's recommendations and make final deletions or additions to the list to take effect January 1 of the next year. He will furnish copies of the list before January 1 to the following:
   (1) physicians licensed by the department;
   (2) directors of clinical laboratories licensed, registered or approved by the department;
   (3) local directors of health in Connecticut;
   (4) health care facilities licensed under Chapter 368v of the Connecticut General Statutes.
(Effective October 25, 1989.)

19a-36-A3. Persons required to report reportable diseases and laboratory findings
(a) Reportable Diseases.
   (1) Every health care provider who treats or examines any person who has or is suspected to have a reportable disease shall report to the local director of health or other health authority within whose jurisdiction the patient resides and to the department such information about the affected person as described in section 19a-36-A4 of these regulations.
   (2) If the case or suspected case of reportable disease is in a health care facility, the person in charge of such facility shall ensure that reports are made to the local director of health and the department in the manner specified in section 19a-36-A4 of these regulations. The person in charge shall designate appropriate infection control or record-keeping personnel for this purpose.
   (3) If the case or suspected case of reportable disease is not in a health care facility and if a health care provider is not in attendance or is not known to have made a report within the appropriate time specified in section 19a-36-A4, such report of reportable diseases shall be made to the local director of health or other health authority within whose jurisdiction the patient lives and the department in the manner specified in section 19a-36-A4 by:
      (A) the administrator serving a public or private school or day care center attended by any person affected or apparently affected with such disease;
      (B) the person in charge of any camp;
      (C) the master or any other person in charge of any vessel lying within the jurisdiction of the state;
      (D) the master or any other person in charge of any aircraft landing within the jurisdiction of the state;
      (E) the owner or person in charge of any establishment producing, handling or processing dairy products, other food or non-alcoholic beverages for sale or distribution;
      (F) morticians and funeral directors.
   (4) Each local director of health shall report or ensure reporting to the department within 24 hours of each case or suspected case of a Category I reportable disease and such additional information of which he has knowledge as described in section 19a-36-A4 of these regulations.
(b) Reportable laboratory findings. - The director of a laboratory that receives a primary specimen or sample which yields a reportable laboratory finding shall be responsible for reporting such findings
Connecticut Department of Public Health – HIV/STD/TB/Hepatitis Surveillance Programs - Confidentiality Guidelines

within forty-eight (48) hours to the local director of health of the town in which the affected person normally resides, or, in the absence of such information, of the town from which the specimen originated, and to the department on forms provided by the department.

(1) When a laboratory identifies or presumptively identifies a significant isolate or other finding that requires confirmation by the laboratory as required in the annual list, the director must submit that isolate or specimen from which the finding was made to the department's laboratory division.

(2) Laboratory tests and confirmatory tests for certain reportable diseases as specially indicated in the annual list shall be exempted from any and all fees for the state laboratory services in accordance with Section 19a-26 of the Connecticut General Statutes.

(Effective October 25, 1989.)

19a-36-A4. Content of report and reporting of reportable diseases and laboratory findings

(a) Reportable diseases.

(1) Each report of a case or suspected case of reportable disease shall include the full name and address of the person reporting and of the physician attending; the diagnosed or suspected disease and date of onset; the full name, age, race/ethnicity, sex and occupation of the affected individual and other facts the department or local director of health requires for purposes of surveillance, control and prevention of reportable diseases. The reports shall be sent in envelopes marked "CONFIDENTIAL."

(2) Reports may be written or oral as required by the category of disease as follows:

(A) Category I: diseases of high priority because of need for timely public health action: reportable immediately by telephone on day of recognition or suspicion of disease; on weekdays to both, the local health director of the town in which the patient resides and the department, on weekends to the department. A completed disease report form provided by the department must also be mailed to both the local health director and the department within 12 hours.

(B) Category II: diseases of significant public health importance, usually requiring public health action: reportable by mail to the local director health and the department within 12 hours of recognition or suspicion on a form provided by the department.

(b) Reportable laboratory findings.

(1) Each report of reportable findings shall include the name, address, age sex, and, if known, race/ethnicity of the person affected, the name and address of the attending physician, the identity of the infectious agent or other reportable laboratory findings, and the method of identification.

(2) Reports shall be mailed to the local director of health of the town in which the patient resides and to the department within 48 hours of making the finding in envelopes marked "CONFIDENTIAL."

(Effective October 25, 1989.)

19a-36-A5. Confidentiality of data

All epidemiologic information which identifies an individual and which is gathered by the state or local health department in connection with the investigation of reported cases or suspected cases of disease or during the investigation of outbreaks of disease shall be kept in compliance with current confidentiality statutes.

(Effective October 25, 1989.)

19a-36-A6. Investigation and control of reportable disease and outbreaks by the department

(a) The department, in cooperation with the local director of health, in the investigation and control of reportable disease shall make or cause to be made such investigation as it deems necessary and shall secure all such data as may assist it in establishing adequate control measures.

(b) In order to investigate and control any apparent outbreak or unusual occurrence of reportable disease, the department shall institute such special disease surveillance, follow-up reports and control measures as it deems necessary.

(c) Individual medical information pertaining to cases of reportable disease, persons affected by outbreaks of disease or significant increases in the rate of nonsocomial infection shall be provided
when requested to an investigator who presents official identification of the department or the local department of health. Such an investigator may be an employee of the State or local health department.

(Effective October 25, 1989.)

19a-36-A7. Diseases not enumerated

Diseases not specifically listed pursuant to section 19a-36-A2 and presenting a special problem shall be reported and controlled in accordance with special instructions of the state department of health or, in the absence of such instructions, in accordance with orders and directions of the local director of health.

(Effective October 25, 1989.)

19a-36-A8. General measures for control of reportable diseases

The local director of health, in instituting measures for the control of reportable diseases:

(a) Investigation shall make, or cause to be made, such investigations as he may deem necessary and shall secure all such data as may assist him in establishing adequate control measures;

(b) Isolation and orders shall establish and maintain quarantine, isolation or such other measures for control as are required by statute, the public health code or special instructions of the state department of health, and, when possible, shall issue his instructions and orders in writing or on printed forms;

(c) Removal shall have the authority to set up proper isolation or quarantine of an affected person or persons, carrier or contact, when, in his opinion or in the opinion of the state commissioner of health, this is not or cannot be effectively maintained on the premises occupied by such person or persons by methods designated in this part; to remove or require the removal of such person or persons to a hospital or other proper place designated by him; or to employ such guards or officers as may be necessary to maintain effective isolation or quarantine;

(d) Instruction shall provide, by himself or his authorized agent, for the specific instruction of cases, contacts, their attendants and all other persons affected, in the proper methods for the prevention of the spread of the disease and shall supply such information and literature as may be required by law or by the instructions of the state department of health;

(e) Enforcement shall make, at intervals during the period of communicability, inquiry or investigation to satisfy himself that the measures instituted by him for the protection of others are being properly observed;

(f) Laboratory tests shall, when the control or release of a case, contact or carrier of a reportable disease is dependent upon laboratory findings, require the specimens upon which such findings are based to be examined by the laboratory division of the state department of health or by a laboratory specifically approved for that purpose by the state department of health and shall, by himself or his authorized agent, secure and submit release cultures or specimens for examination; in cases of enteric diseases all release specimens shall be taken at least one week after specific therapy has been discontinued;

(g) Schools - Isolation shall, in the event of an outbreak of a communicable disease in any public, private, parochial or church school, make a prompt and thorough investigation; control such an outbreak by individual examination of pupils, teachers and other persons associated with the outbreak; employ such other means as he deems necessary to determine the source of infection or to provide for the segregation of infected persons; in the event of an outbreak of a communicable disease in any school, require school physicians and school nurses to conform to the orders, regulations and restrictions issued by him;

(h) Schools - Readmission shall, in the case of any school child who has been excluded from school for having been a case, contact or carrier of a communicable disease, by himself or his authorized agent, issue a permit for such child to re-enter school when in his opinion such child is no longer infectious;

(i) Unusual disease shall, when an unusual or rare disease occurs in any part of the state or when any disease becomes so prevalent as to endanger the state as a whole, contact the state department of health for assistance, and shall cooperate with the representatives of the state department of health acting under the direction of the state commissioner of health;

(j) Other measures shall introduce such other measures as he may deem advisable.

(Effective October 25, 1989.)
Appendix 2:

Disclosure of Health Data

19a-25-1. Definitions
As used in Sections 19a-25-1 through 19a-25-4, inclusive, of the Regulations of Connecticut State Agencies:

(1) "Aggregate health data" means health data that is obtained by combining like data in a manner that precludes the identification of the individual or organization supplying the data or described in the data.

(2) "Anonymous medical case history" means the description of an individual's illness in a manner that precludes the identification of the individual or organization supplying the data or described in the data.

(3) "Commissioner" means the commissioner of the Department of Public Health.

(4) "Department" means the Department of Public Health.

(5) "Disclosure" or "disclose" means the communication of health data to any individual or organization outside the department.

(6) "Health data" means information, recorded in any form or medium, that relates to the health status of individuals, the determinants of health and health hazards, the availability of health resources and services, or the use and cost of such resources and services.

(7) "Identifiable health data" means any item, collection, or grouping of health data that makes the individual or organization supplying it, or described in it, identifiable.

(8) "Individual" means a natural person.

(9) "Local Director of Health" means the city, town, borough, or district Director of Health or any person legally authorized to act for the local director of health.

(10) "Medical or scientific research" means the performance of activities relating to health data, including, but not limited to:

(A) describing the group characteristics of individuals or organizations;
(B) characterizing the determinants of health and health hazards;
(C) analyzing the inter-relationships among the various characteristics of individuals or organizations;
(D) the preparation and publication of reports describing these matters; and
(E) other related functions as determined by the commissioner.

(11) "Organization" means any corporation, association, partnership, agency, department, unit, or other legally constituted institution or entity, or part thereof.

(12) "Studies of morbidity and mortality" means the collection, application, and maintenance of health data on:

(A) the extent, nature, and impact of illness and disability on the population of the state or any portion thereof;
(B) the determinants of health and health hazards, including but limited to,
   (i) infectious agents of disease,
   (ii) environmental toxins or hazards,
   (iii) health resources, including the extent of available manpower and resources, or
   (iv) the supply, cost, financing or utilization of health care services.
(C) diseases on the commissioner's list of reportable diseases and laboratory findings pursuant to section 19a-215 of the Connecticut General Statutes; or
(D) similar health or health related matters as determined by the commissioner.

(Effective October 30, 1998.)

19a-25-2. Disclosure of aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality
(a) The department may, at the discretion of the commissioner, publish, make available, and disseminate aggregate health data, anonymous medical case histories, and reports of the findings of studies of morbidity and mortality, provided such data, histories, and reports:

(1) Are prepared for the purpose of medical and scientific research; and

(2) Do not include identifiable health data.

(b) No individual or organization with lawful access to such reports shall be compelled to testify with regard to such reports. Publication or release of such reports shall not subject said report or related information to subpoena or similar compulsory process in any civil or criminal, judicial, administrative or legislative proceeding.


19a-25-3. Disclosure of identifiable health data

(a) The department shall not disclose identifiable health data unless:

(1) The disclosure is to health care providers in a medical emergency as necessary to protect the health, life, or well-being of the person with a reportable disease or condition pursuant to section 19a-215 of the Connecticut General Statutes;

(2) The disclosure is to health care providers, the local director of health, the department, another state or public health agency, including those in other states and the federal government, or other persons when deemed necessary by the department in its sole discretion for disease prevention and control pursuant to section 19a-215 of the Connecticut General Statutes or for the purpose of reducing morbidity and mortality from any cause or condition, except that every effort shall be made to limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose;

(3) The disclosure is to an individual, organization, governmental entity in this or another state or to the federal government, provided the department determines that:

(A) Based upon a written application and such other information as required by the department to be submitted by the requesting individual, organization or governmental entity the data will be used solely for bona fide medical and scientific research;

(B) The disclosure of data to the requesting individual, organization or governmental entity is required for the medical or scientific research proposed;

(C) The requesting individual, organization, or governmental entity has entered into a written agreement satisfactory to the department agreeing to protect such data in accordance with the requirements of this section and not permit disclosure without prior approval of the department; and

(D) The requesting individual, organization or governmental entity, upon request of the department or after a specified date or event, returns or destroys all identifiable health data provided by the department and copies thereof in any form.

(4) The disclosure is to a governmental entity for the purpose of conducting an audit, evaluation, or investigation required by law of the department and such governmental entity agrees not to use such data for making any determination as to whom the health data relates.

(b) Any disclosure provided for in this section shall be made at the discretion of the department, provided the requirements for disclosure set forth in the applicable provisions of this section have been met. For disclosures under this section to governmental entities, the commissioner may waive the requirements of this section except for the requirements of subdivision (A) of subsection (3).

(c) Notwithstanding any other provisions of this section, no identifiable health data obtained in the course of activities undertaken or supported under this section shall be subject to subpoena or similar compulsory process in any civil or criminal, judicial, administrative, or legislative proceeding, nor shall any individual or organization with lawful access to identifiable health data under the provisions of this section be compelled to testify with regard to such health data.

(Effective October 30, 1998.)
19a-25-4. Use of health data for enforcement purposes

(a) Notwithstanding any provisions of sections 19a-25-1 to 19a-25-3, inclusive of the Regulations of State Agencies, the department may utilize, in any manner, health data including but not limited to aggregate health data, identifiable health data, and studies of morbidity and mortality, in carrying out and performing its statutory and regulatory responsibilities and to secure compliance with or enforcement of any laws. Where such data is used in an enforcement action brought by the department or any other state agency, disclosure to parties to the action of such data shall be permitted only if required by law and said parties may not further disclose such data except to a tribunal, administrative agency or court with jurisdiction over the enforcement action. Disclosure under this section does not constitute a waiver or release of the confidentiality that protects such data.

(Effective October 30, 1998.)
Appendix 3:

**Federal Assurance of Confidentiality**

“The national surveillance program for HIV/AIDS is being coordinated by the Centers for Disease Control (CDC), an agency of the Public Health Service (USPHS). The surveillance information requested by CDC consists of reports of persons with suspected or confirmed HIV infection and AIDS. The data are used for statistical summaries and research by USPHS scientists and cooperating state and local health officials to help understand and control the spread of HIV/AIDS.

Information in the surveillance system that would permit identification of any individual on whom a record is maintained is collected with guarantee that it will be held in strict confidence, will be used only for the purposes stated in the assurance, and will not otherwise be disclosed or released without consent of the individual in accordance with Section 306 and 308(d) of the Public Health Service Act (42 U.S.C. 242k and 242m(d)).

Information you provide that could be used to identify any individual on whom a record is maintained will be kept confidential. Full names, addresses, social security numbers, and telephone numbers will not be reported to this national surveillance system. Medical, personal, and lifestyle information about the case, the birth date, and alpha-numeric code based on surname will be used.

Surveillance information reported to CDC will be without identifiers primarily for statistical and analytical summaries in which no individual on whom a record is maintained can be identified and, secondarily, for special investigations of the natural history and epidemiology of HIV/AIDS. When necessary for confirming surveillance information or in the interest of public health and disease prevention, the CDC may confirm information contained in case reports or may notify other medical personnel or health officials of such information; in each instance, only the minimum information necessary will be disclosed.

Collaborative research efforts with an important public health purpose will require approval by the Director of CDC pursuant to strict conditions. If disclosure of identifying information to the collaborating researchers is essential to conduct of the research, a written certificate will be required stating that identifying information obtained from CDC will be managed as confidential and will not be released or redisclosed.

No CDC HIV/AIDS surveillance information that could be used to identify individual on whom a record is maintained, either directly or indirectly, will be made available to anyone for nonpublic health purposes. In particular, such information will not be disclosed to the public, parties involved in civil, criminal, or administrative litigation, or non-health agencies of the federal, state, or local government.”
Appendix 4:

STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

HIV/STD/TB/Hepatitis Surveillance

Confidentiality Agreement (Revised December 2014)

I, (print name) ____________________________________________, have read and had an opportunity to ask questions about Connecticut Regulation19a-25 and the current version of the Connecticut Department of Public Health (DPH) HIV/STD/TB/Hepatitis Confidentiality Guidelines. I understand and will comply with the requirements therein. I understand that failure to adhere to these requirements could result in administrative or legal action.

I agree

• Not to communicate personally identifiable information (PII/PHI) to others except as necessary to conduct DPH-authorized work (including any information maintained by DPH that can be used to distinguish an individual such as name, mother’s maiden name, street address, date/place of birth, social security number, medical record number; and, other information that is linkable to an individual, such as medical, educational, financial, and employment information);

• To protect encryption keys, passwords, and other security access codes from release to unauthorized persons and protect computers, servers, laptops, mobile devices, and storage media for which I am responsible from unauthorized access, loss, or theft;

• Not to enable others to gain access to PII/PHI who are not authorized by the Program Coordinator;

• Not to remove PII/PHI from my worksite except when authorized by the Program Coordinator;

• To report to the immediate supervisor breaches or suspected breaches of confidentiality protocol or loss of PII/PHI.

Signed

Employee or contractor: ___________________________ Role: ___________________________

Date/Training date: ______________ Section/Program: ___________________________

Program Coordinator: ___________________________ Date: ___________________________
Appendix 5:

PURPOSE:

The purpose of this policy and procedure at the Connecticut Department of Public Health (DPH) is to maintain a safe and secure work environment for its employees. All DPH employees are required to comply with the safety procedures outlined below.

SCOPE:

This policy and procedure applies to all DPH employees at the Capitol Avenue complex.

DEFINITIONS:

N/A

POLICY:

The Security Protocols policy at the Connecticut DPH is to maintain a safe and secure work environment for its employees.

PROCEDURES:

1. Employees must visibly display a State issued photo identification (ID) badge at all times when present at the 410-470 Capitol Avenue complex.
2. If a State photo ID badge is unavailable upon entering the complex, employees must produce a valid ID (Connecticut driver’s license, passport) and sign-in at the security desk to obtain a visitor’s pass. This pass must be worn throughout the day while in the complex.
3. If a State ID badge is lost, employees must contact Human Resources to arrange for a replacement ID badge.
4. Security doors are to be completely closed after entering and leaving the building complex.
Appendix 6: HIPAA Access Letter

Access letter for field epidemiologists reviewing medical records:

STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

To: Health care provider or Medical Records Department Staff

From: Heidi Jenkins, Section Chief, Hepatitis, HIV, STD and TB Section

Date: December 19, 2016

Re: Access to medical records and/or patient information

[Insert name] is authorized to review patient medical records or have access to patient information regarding reportable diseases or conditions on behalf of the Connecticut Department of Public Health (DPH). Covered entities may release personally identifiable health information to the Department and its agents without an authorization, consent, release, or opportunity to object by the patient under both state and federal (HIPAA) law, as follows: Pursuant to Conn. Gen. Stat. §§19a-215 and the Regulations of State Agencies §§19a-36-A4 and 19a-36-A6, the requested information is required to be provided to the Department of Public Health and its agents. Please note that Conn. Gen. Stat. §§52-1450(b)(1) authorizes the release of these records without the patient’s consent.

Additionally, the Department of Public Health is a health oversight agency as defined by §164.501 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA also authorizes providers to release personally identifiable health information to the Department without an authorization, consent, release, or opportunity to object by the patient, as information (i) required by law to be disclosed (HIPAA Privacy Regulation, 42 CFR §164.512(a)), (ii) as part of the Department’s public health activities (HIPAA Privacy Regulation, 42 CFR §164.512(b)), and (iii) as part of the Department’s public health oversight activities (HIPAA Privacy Regulation, 42 CFR §164.512(d)). Please note: the definition of “health oversight agency” (§164.501 of HIPAA Privacy Regulations) includes entities “acting under a grant of authority from or contract with such public agency.” Thus, covered entities are authorized to release personally identifiable health information under the authorities cited above, to the Department’s contractors who are acting as the Department’s agents.

Providers may also rely upon the Department’s and its agent’s representations that the requested information is what is minimally necessary to achieve the purpose of the disclosure (42 CFR §164.514(c)(3)(iii)(A) of the HIPAA Privacy Regulations).

The medical records department or provider office may wish to retain a copy of this letter and attachments as well as a copy of the DPH picture ID card of the person presenting this letter.

Thank you very much for your cooperation.
Appendix 7: Retention Schedule

(First page of the retention schedule for HIV surveillance related forms.)

<table>
<thead>
<tr>
<th>RECORDS RETENTION SCHEDULE</th>
<th>STATE OF CONNECTICUT</th>
<th>RECORDS RETENTION SCHEDULE #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of Public Health - Infectious Disease Unit</td>
<td>Connecticut State Library</td>
<td>13-1-2</td>
</tr>
<tr>
<td>Form RC-050 (Revised 07/2012)</td>
<td>Office of the Public Records Administrator</td>
<td></td>
</tr>
<tr>
<td>460 Capitol Avenue, Hartford, CT 06106</td>
<td>231 Capitol Avenue, Hartford, CT 06106</td>
<td></td>
</tr>
<tr>
<td>AGENCY: Department of Public Health (DPH)</td>
<td>AGENCY ADDRESS:</td>
<td>This schedule is:</td>
</tr>
<tr>
<td>DIVISION, UNIT, OR FUNCTION: Infectious Disease Unit</td>
<td>460 Capitol Avenue, Hartford, CT 06106</td>
<td>☐ ORIGINAL</td>
</tr>
<tr>
<td>RELEVANT STATUTES &amp; REGULATIONS AND ACRONYMS USED ON THIS SCHEDULE: Connecticut General Statutes §19a-2a thru 19a-215; Public Health Code §9a-36-A3 thru 19a-36-A4</td>
<td></td>
<td>☐ REVISED</td>
</tr>
<tr>
<td>RMLO (type or print): Lisa Kedler</td>
<td>SUPERSEDED SCHEDULE NUMBER(S):</td>
<td></td>
</tr>
<tr>
<td>JOB TITLE OF RMLO (type or print): Staff Attorney</td>
<td>N08-4-2, Epidemiology (p. 2), STD (p. 3), and Pulmonary (p. 4)</td>
<td></td>
</tr>
<tr>
<td>APPROVED (Signature of Archivist):</td>
<td>DATE SIGNED:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9/26/2013</td>
<td></td>
</tr>
<tr>
<td>APPROVED (Signature of Public Records Administrator):</td>
<td>EFFECTIVE DATE OF SCHEDULE:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9/26/2013</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Series #</th>
<th>Records Series Title</th>
<th>Description</th>
<th>Retention</th>
<th>Disposition</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. INFECTIOUS DISEASE SECTION (Administration)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01. Annual Disease Reports</td>
<td>This series documents infectious disease statistics from 1890 to present. Data are arranged by town and disease and by year. The report includes, but is not limited to: Epidemiology, Sexually Transmitted Diseases (STD) and Tuberculosis.</td>
<td>Permanent</td>
<td>Retain in agency or transfer to State Archives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>02. Annual Disease Summary</td>
<td>This series summarizes infectious disease statistics by disease and by year from 1890 to present. This report is inclusive, but not limited to: Epidemiology, Sexually Transmitted Diseases (STD) and Tuberculosis.</td>
<td>Permanent</td>
<td>Retain in agency or transfer to State Archives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B. EPIDEMIOLOGY AND EMERGING INFECTIONS PROGRAM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>03. Reportable Disease and Outbreak Investigation Files</td>
<td>This series documents the investigation of reportable diseases and outbreaks pursuant to Conn. Agencies Regs. §19a-36-A5; including but not limited to: written reports, surveys including prevalence studies, background materials, questionnaires, databases and previous studies.</td>
<td>10 years from the date DPH is informed of an outbreak</td>
<td>Destroy after receipt of signed Form RC-108</td>
<td>The date the DPH is informed of an outbreak is the date to be used as the start date of the outbreak.</td>
<td></td>
</tr>
<tr>
<td>Series #</td>
<td>Records Series Title</td>
<td>Description</td>
<td>Retention</td>
<td>Disposition</td>
<td>Notes</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>04.</td>
<td>Reportable Disease Forms</td>
<td>This series documents diseases reported by persons or laboratories required to report certain illnesses and infectious agents in accordance with Connecticut Public Health Law. It includes laboratory evidence of a communicable disease, as well as reports of deaths and hospital discharges among certain groups.</td>
<td>3 years from date reported</td>
<td>Destroy after receipt of signed Form RC-508</td>
<td>The date the DPH is informed of an outbreak is the date to be used as the start date of the outbreak.</td>
</tr>
<tr>
<td>05.</td>
<td>Reportable Disease and Outbreak Investigation Files</td>
<td>This series documents the investigation of reportable diseases and outbreaks pursuant to Connecticut Agencies Regs. Sections 139a-36-A6. It includes, but is not limited to, supporting documentation including surveys, background materials, questionnaires, databases, and previous studies.</td>
<td>1 year from the date DPH is informed of an outbreak</td>
<td>Destroy after receipt of signed Form RC-508</td>
<td>The date the DPH is informed of an outbreak is the date to be used as the start date of the outbreak.</td>
</tr>
<tr>
<td>06.</td>
<td>Reportable Disease Special Research Projects</td>
<td>This series documents research projects, including, but not limited to, Lyme disease, emerging infections, other federally or outside funded, including, but not limited to, Yale Emerging Infections Program. It includes, but is not limited to, surveys, background materials, questionnaires, databases, and previous studies.</td>
<td>3 years after DPH notification of outbreak</td>
<td>Destroy after receipt of signed Form RC-508</td>
<td>The date the DPH is informed of an outbreak is the date to be used as the start date of the outbreak.</td>
</tr>
<tr>
<td>C.</td>
<td>HEALTHCARE ASSOCIATED INFECTIONS (HAI) PROGRAM</td>
<td>This series documents data collected during chart audits of health facility patients who may be eligible to be reported to DPH as a case of healthcare associated infection. These records are distinct from standard reportable disease forms. They are used to determine the accuracy and completeness of healthcare facility reporting of publicly reportable HAIs.</td>
<td>3 years</td>
<td>Destroy after receipt of signed Form RC-508</td>
<td>The date the DPH is informed of an outbreak is the date to be used as the start date of the outbreak.</td>
</tr>
</tbody>
</table>
**RECORDS RETENTION SCHEDULE**

**Department of Public Health - Infectious Disease Unit**

**Form RC-050 (Revised 02/2012)**

<table>
<thead>
<tr>
<th>Series #</th>
<th>Records Series Title</th>
<th>Description</th>
<th>Retention</th>
<th>Disposition</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>08.</td>
<td>Annual Public Health Reports to the Legislature</td>
<td>This series documents legislatively mandated annual reports to the chairs of the Public Health Committee summarizing data on publicly reportable HIVs in healthcare facilities in Connecticut.</td>
<td>Permanent</td>
<td>Retain in agency</td>
<td>These reports are also posted to the DPH website pursuant to C.G.S. § 19a-400a. The agency also retains the records of Advisory Committee on Healthcare Associated Infections established by C.G.S. § 19a-489b. See 51 for retention requirements.</td>
</tr>
</tbody>
</table>

**D. SEXUALLY TRANSMITTED DISEASE (STD) PROGRAM**

<table>
<thead>
<tr>
<th>Series #</th>
<th>Records Series Title</th>
<th>Description</th>
<th>Retention</th>
<th>Disposition</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>09.</td>
<td>STD Case Reporting Forms</td>
<td>This series documents sexually transmitted diseases reported by persons or laboratories required to report or where laboratory evidence suggests an STD. Includes but is not limited to STD Case Report (STD-23) and Laboratory Report of Significant Findings (OL-15C) that are specific for STIs.</td>
<td>3 years</td>
<td>Destroy after receipt of signed Form RC-108</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>STD Epidemiological Records</td>
<td>This series documents reports to the federal Center for Disease Control (CDC) of individual cases of STDs including Syphilis. Includes but is not limited to field and interview records used to gather information on individual patients.</td>
<td>3 years</td>
<td>Destroy after receipt of signed Form RC-108</td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Syphilis Case Reports, Monthly</td>
<td>[Obsolete] This series documents internal program monthly and annual summaries of syphilis cases reported in the state, 2000 - 2010.</td>
<td>3 years</td>
<td>Destroy after receipt of signed Form RC-108</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>STD Summary Morbidity Reports</td>
<td>[Obsolete] This series documents summaries of STD cases diagnosed in the state as well as quarterly and annual reports made to CDC. This includes but is not limited to STD Quarterly/Annual Morbidity Report, Annual Report, Civilian Cases of Syphilis, Secondary and Early Latent Syphilis and Gonorrhea and Quarterly Epidemiological Activity for Venereal Disease Report.</td>
<td>Permanent</td>
<td>Retain in agency or transfer to State Archives</td>
<td></td>
</tr>
<tr>
<td>Series #</td>
<td>Records Series Title</td>
<td>Description</td>
<td>Retention</td>
<td>Disposition</td>
<td>Notes</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>13.</td>
<td><strong>TUBERCULOSIS (TB) CONTROL PROGRAM</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13. <strong>Patient Files, Active TB (Numerical)</strong></td>
<td>This series documents information for patients diagnosed with tuberculosis disease. This includes but is not limited to physician and laboratory report forms, clinical information, contact investigation forms and master index cards with medication information.</td>
<td>10 years onsite; 60 years offsite</td>
<td>Destroy after receipt of signed Form RC-100</td>
<td>*It is necessary to retain TB patient records for up to 70 years because persons who have latent TB infection or TB disease have a life-time risk of developing active TB or recurrent TB.</td>
</tr>
<tr>
<td></td>
<td>14. <strong>Patient Files, Latent TB (Alphabetical)</strong></td>
<td>This series documents information for patients diagnosed with latent tuberculosis infection. This includes but is not limited to physician and laboratory report forms, clinical information, contact investigation forms and master index cards with medication information.</td>
<td>10 years onsite; 60 years offsite</td>
<td>Destroy after receipt of signed Form RC-100</td>
<td>*It is necessary to retain TB patient records for up to 70 years because persons who have latent TB infection or TB disease have a life-time risk of developing active TB or recurrent TB.</td>
</tr>
<tr>
<td></td>
<td>15. <strong>Patient Files, Active TB – Master Index Cards</strong></td>
<td>[Obsolete] This series documents a variety of finding aids for access to files of patients with diagnosed tuberculosis disease.</td>
<td>10 years onsite; 60 years offsite</td>
<td>Destroy after receipt of signed Form RC-100</td>
<td>The master card indexes end in 2013 when the last file index was computerized.</td>
</tr>
<tr>
<td></td>
<td>16. <strong>Verified TB Cases Reports</strong></td>
<td>This series documents reports to the federal Center for Disease Control (CDC) of individual tuberculosis cases.</td>
<td>3 years</td>
<td>Destroy after receipt of signed Form RC-100</td>
<td></td>
</tr>
<tr>
<td></td>
<td>17. <strong>Federal Grant / Programmatic Materials</strong></td>
<td>This series documents federal program and grant management. This includes but is not limited to grant and program activity reports made to CDC.</td>
<td>3 years from the date of the last expenditure report submitted for the funding period (45 CFR 92.42)</td>
<td>Destroy after receipt of signed Form RC-100</td>
<td></td>
</tr>
<tr>
<td></td>
<td>18. <strong>Refugee Health Assessment Records</strong></td>
<td>This series documents medical follow-up for persons entering Connecticut as refugees. This includes but is not limited to health care provider forms and test results.</td>
<td>10 years</td>
<td>Destroy after receipt of signed Form RC-100</td>
<td></td>
</tr>
<tr>
<td></td>
<td>19. <strong>Refugee Arrival Forms/Class A/B Immigrant Arrival Forms</strong></td>
<td>This series documents information received informing the state of refugees and immigrants arriving in Connecticut with overseas TB classifications that require medical and public health follow-up. This includes but is not limited to notification forms and support documents from CDC and other organizations.</td>
<td>3 years</td>
<td>Destroy after receipt of signed Form RC-100</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 8: Fax Disclaimer

Sample Confidentiality Disclaimer

The documents accompanying this fax transmission contain health information that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its stated need has been fulfilled. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.

* Based on “Facsimile Transmission of Health Information”
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031811.hcsp?dDocName=bok1_031811
Appendix 9. PCSI Disaster Recovery Plan

CONNECTICUT DEPARTMENT OF PUBLIC HEALTH

PCSI DISASTER RECOVERY PLAN

Contacts:

Rory Angulo MD, MBA (HIV)
(860) 509-7900
rory.angulo@ct.gov

Heidi Jenkins (STD, TB, HIV, Hepatitis)
(860) 509-7924
heidi.jenkins@ct.gov

410 Capitol Avenue
PO Box 340308
Hartford CT 06134-0308

Last updated: November 29, 2016
# Table of Contents

Introduction ................................................................................................................................................. 3

Plan scope.................................................................................................................................................. 3

1. Disaster Recovery Lead .......................................................................................................................... 4
2. Disaster Recovery Teams & Responsibilities ......................................................................................... 4
3. Other teams as set forth in DPH IT DRP ............................................................................................... 5
4. Critical Vendors and RTO ..................................................................................................................... 5
5. DRP Activation ...................................................................................................................................... 5
6. Disaster Recovery call tree .................................................................................................................... 6
7. Version information & Changes ........................................................................................................... 7
Introduction

A disaster can be defined as an scenario caused by man or of natural origin that result in PCSI program staff activities not being able to perform all or some of their normal activities and responsibilities due to physical damage of servers at DPH IT.

The following events can cause disaster that would require the activation of PCSI DR plan: Fire, water damage, power outage and theft.

Purpose of the PCSI disaster recovery plan is to mitigate the impact of incidents that generate massive loss of electronic data or its access to restricted confidential information with the ultimate goal to resume and maintain business continuity for PCSI program activities.

This plan shall be used as an initial response to a disaster, as declared by PCSI coordinator or data security manager that require the restoration of data files and/or application services. This document shall be succeeded by DPH IT DRP actions when in conflict or areas not included in this document.

Plan scope

This document shall address steps to follow in the event PCSI programs are affected by the loss of data files or applications caused by the physical damage to servers located at 410 Capitol building and maintained by DPH IT staff.

The following areas will be considered when PCSI DR is activated

1. Disaster Recovery Lead
2. Disaster Recovery Teams & Responsibilities.
3. Other teams.
4. Disaster Recovery call tree.

This DRP does not take into consideration issues related to human resources and real estate related disaster. Please contact PCSI program coordinator or confidentiality manager for issues not observed in this document.
1. Disaster Recovery Lead

The Disaster Recovery lead team is tasked with the decision to declare an incident as a disaster that requires the activation of the PCSI DR plan. The team will guide and coordinate/collaborate with PCSI and DPH IT staff in the recovery process. PCSI staff will report to the team and to the joint IT lead team, when convened. Lead team members shall not be part of other DR groups in the CT DPH.

Contact information

<table>
<thead>
<tr>
<th>Name</th>
<th>Role/ Title</th>
<th>work phone number</th>
<th>home phone number</th>
<th>mobile phone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heidi Jenkins</td>
<td>PCSI primary lead</td>
<td>(860)509-7924</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rory Angulo</td>
<td>PCSI secondary lead</td>
<td></td>
<td>(860)509-7691</td>
<td></td>
</tr>
<tr>
<td>Eva Golebiewski</td>
<td>DPH IT primary lead</td>
<td></td>
<td>(860)509-7430</td>
<td></td>
</tr>
<tr>
<td>Nicholas Piscatelli</td>
<td>DPH IT secondary lead</td>
<td></td>
<td>(860)509-8145</td>
<td></td>
</tr>
</tbody>
</table>

2. Disaster Recovery Teams & Responsibilities

In the event of a disaster, PCSI primary/secondary lead will require assistance from IT and other groups to work on restoration of normal functionality of PCSI database, applications and file systems.

Contact information

<table>
<thead>
<tr>
<th>Name</th>
<th>Role/ Title</th>
<th>work phone number</th>
<th>home phone number</th>
<th>mobile phone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carl Bondeson</td>
<td>Applications/ data restore</td>
<td>(860)509-7434</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gobi Natarajan</td>
<td>Applications/ data restore</td>
<td>(860)509-7217</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. **Other teams as set forth in DPH IT DRP**

Other teams, not considered in this document shall be activated by DPH IT lead as deemed necessary to mitigate the disaster and restore PCSI program and staff functionality.

4. **Critical Vendors and RTO**

DPH agency electronic data is backed up on a nightly basis. A media containing the data is transported on a weekly basis to an off-site contractor location. Upon activation of DR plan, contractor must be contacted to prepare media and devices that are required to complete needed data restoration task. DPH IT team will lead this task and sign off on documents to track location of media/devices upon arrival to agency. Contractors will provide recovery time objective when requested.

<table>
<thead>
<tr>
<th>Name</th>
<th>Role/Title</th>
<th>Work Phone Number</th>
<th>Home Phone Number</th>
<th>Mobile Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. **DRP Activation**

Once PCSI team lead, or jointly agency or DPH IT team lead, declares a disaster that requires the activation of the DRP, team lead(s) will initiate the activations of the DRP by triggering the DR call tree.

The team lead will consider the following topics in all related calls for the duration of the DRP activation:

- *That a disaster has occurred*
- *The nature of the disaster (if known)*
- *The initial estimation of the magnitude of the disaster (if known)*
- *The initial estimation of the impact of the disaster (if known)*
- *The initial estimation of the expected duration of the disaster (if known)*
- *Actions that have been taken to this point*
- *Actions that are to be taken prior to the meeting of Disaster Recovery Team Leads*
- *Scheduled meeting place for the meeting of Disaster Recovery Team Leads*
- *Scheduled meeting time for the meeting of Disaster Recovery Team Leads*
- *Any other pertinent information*
6. Disaster Recovery call tree

PCSI lead team will notify DPH IT lead team or any other activated DPH DR Management team of a disaster, from the list above, that is impacting PCSI normal operations.

DPH IT lead team or DPH DR Management team will in turn activate other teams under their supervision and as described in DPH IT DR plan to help mitigate and restore agency or PCSI regular activities.

7. Version information & Changes

Please log any changes made to this document by filling in all fields below

<table>
<thead>
<tr>
<th>Name of person making changes</th>
<th>Role of person making changes</th>
<th>Date of change</th>
<th>Version number</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rory Angulo</td>
<td>PCSI 2nd lead</td>
<td>12/17/2014</td>
<td>1.0</td>
<td>Initial version</td>
</tr>
<tr>
<td>Rory Angulo</td>
<td>PCSI 2nd lead</td>
<td>11/29/2016</td>
<td>1.1</td>
<td>Contact information update</td>
</tr>
</tbody>
</table>

Comments

- save a copy of this document at the following locations:
  - in the HIV directory ‘X:\security\confidentiality manual’
  - in the shared drive ‘U:\SHAREDOC\PCSI docs_gen’
- Notify team leads of document updates.
Appendix 10.

Fillable form can be found at: U:\SHAREDOC\DPH Forms\ IT Mobile Data Control Form .docx (CTDPH-intranet)

State of CT-Department of Public Health
Information Technology
Phone: 860-509-7777
Email: Helpdesk.DPH@ct.gov
410 Capitol Avenue, 3rd Floor, MS #13DPR
Hartford, CT 06134

**MOBILE DATA CONTROL FORM**

Please submit completed form to Helpdesk.dph@ct.gov

**Date:** Click here to enter a date.

**Requester Name:** Click here to enter text.  
**Phone Number:** Click here to enter text.

**Email Address:** Click here to enter text.

| Mobile device on which data will be stored (list only one device per form) |
|-------------------------------------------------|-------------------------------------------------|
| **Serial Number:** Click here to enter text. | **Asset Tag Number:** Click here to enter text. |

**Date to be transferred to device:** Click here to enter a date.

<table>
<thead>
<tr>
<th>Source System Name</th>
<th>Data Source Table/File Identifiers</th>
<th>Description of Data</th>
<th>Level of Sensitivity</th>
<th>Business need for Transfer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click here to enter text.</td>
<td>Click here to enter text.</td>
<td>Click here to enter text.</td>
<td>Click here to enter text.</td>
<td>Click here to enter text.</td>
</tr>
</tbody>
</table>

The signer below certifies:

- No reasonable alternative means exists to securely access requested data;
- The business need for storing this data on the designated mobile device outweighs associated risks and all such risks are accepted.

**Approved by:**

________________________________________
Signature, Title, Date
Data Owner

Data transfer request is acknowledged and granted as specified:

Click here to enter text.

Approved by:

Signature, Title, Date

Print Full Name  Click here to enter text.

User

By my signature below, I understand and agree to abide by the State of Connecticut Department of Information Technology Policy on Security for Mobile Computing and Storage Devices:

Signature, Title, Date

Print Full Name  Click here to enter text.

Final Disposition

Complete this section when data identified is no longer authorized for use on mobile device identified on this form.

I, the undersigned, attest that all requested data has been removed from the device identified on this form in accordance with current State of Connecticut practices and procedures.

User  IT Asset Manager

Signature, Title, Date  Signature, Title, Date