STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

Policy Name:	Data Security Breach Involving Non-Laboratory Data	**Number:**	LO-04-000
Procedure:	See page 2		
Applies to:	All DPH Employees and DPH programs, Except for the Laboratory		
Position Responsible:	General Counsel		
Effective Date:	12/16/2019	**Last Reviewed:**	
Approved		**Date**	12/16/2019

PURPOSE:

This statement of policy is intended to carry out the Department of Public Health's ("Department") responsibilities under federal law, the Connecticut General Statutes (the "Statutes" or "C.G.S"), and applicable Regulations of Connecticut State Agencies (the "Regulations") in protecting the confidential data collected and housed at the Department.

SCOPE:

This policy applies to all employees and contractors, including but not limited to student interns, federal or state employees placed at DPH, interim and durational employees of the Department and all the programs that collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal health information or personally identifiable information of the citizens of Connecticut and employees of the Department.

DEFINITIONS:

A. Data security breach, in accordance with § 36a-701b of the Statutes, is the unauthorized access to and acquisition of unencrypted and un-redacted records or data containing personal information where illegal use of personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to an individual. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information by an employee or agent of the Department for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose and is not subject to further unauthorized disclosure.
B. In the case of the Department of Public Health, a data security breach is the unauthorized disclosure and access of Department of Public Health confidential information such as personal health information ("PHI") or personal identifiable information ("PII") stored and

maintained at the Department of Public Health in accordance with applicable statutes and regulations.

C. "Personal data". In accordance with § 4-190(9) of the Statutes, personal data is "any information about a person's education, finances, medical or emotional condition or history, employment or business history, family or personal relationships, reputation or character which because of name, identifying number, mark or description can be readily associated with a particular person." Personal data shall not be construed to make available to a person any record described in subdivision (3) of subsection (b) of section 1-210.

D. "Disclosure' or 'disclose' means the communication of health data to any individual or organization outside the [D]epartment," (§ 19a-25-1(5) of the Regulations), or communication to any individual within the Department who does not have specific authority to access the health data.

E. "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. § 19a-25-1(6) of the Regulations.

F. "Identifiable health data" or 'identifiable health information" means any item, collection, or grouping of health data that makes the individual or organization supplying it, or described in it, identifiable." § 19a-25-1(7) of the Regulations.

G. "Protected Health Information [PHI]" means individually identifiable health information. 45 CFR § 160.103.

H. Data Security Officer- a person assigned to investigate data breach incidents, and review and/or issue data-breach reports.

POLICY:

This policy provides a procedure and process for the protection and mitigation of damages in the event that personal health information or non-public personal information (the data included in the Definition Section of this Data Breach Policy) becomes compromised by a security breach that may lead to identity theft and invasion of privacy for affected individuals. In the event of a data security breach, the Department will take specific steps as outlined in the Procedures and Process sections of this policy.

PROCEDURES:

I. **Implementing Safeguards**

All programs must implement the following safeguards:

- Require all employees to notify their supervisors immediately of any actual or suspected security breach involving files containing non-public personal information. For example, a breach may involve a lost or stolen computer or other device containing unencrypted non-public personal information or the access of non-public personal information by unauthorized individuals. If employees are uncertain whether there has been a breach, they must be advised to report the event to their supervisors.

- Regularly train employees, including all temporary, contract, or work-study interns, to take basic steps to maintain the security, confidentiality and integrity of personal information:
    - Locking rooms and file cabinets where paper records are kept
    - Using password-activated screensavers
    - Using unique passwords
    - Changing passwords periodically and not posting passwords on employees' computers
    - Never sharing passwords with others
    - Encrypting non-public personal information when it is transmitted electronically over networks or stored on-line
    - Referring calls or other request for non-public personal information to designated individuals within the Department
    - Requiring all vendors/contractors having access to non-public personal data to take all necessary steps in protecting and handling any such data, including, but no limited to developing their own policies, procedures and systems to protect the confidentiality, security, integrity of such data and to detect the occurrence of a data breach. This requirement must be imposed on vendors/contractors by a written provision in contracts.

II. Reporting of Data Security Breach

Any time an employee discovers or suspects a data security breach, the employee must immediately report such information to the supervisor. Supervisor must immediately report the actual or suspected security breach to Section/Branch Chief, and then to the Data Security Officer.

III. Risk Assessment

The Data Security Officer will perform a risk assessment and determine whether a data security breach has occurred, determine the causes of the breach, and take immediate steps to mitigate damages.

The Data Security Officer will document date of breach, the name and contact information of the person reporting the breach, type of data included in the breach, causes of the breach occurred, individuals affected, type of data affected, mitigating steps taken,

<u>Specifically, the Data Security Officer shall document</u>:

- <u>Identification</u>:
    - The party, if identifiable, that obtained/accessed the non-public information.
    - The party at fault for the breach.
    - The party who discovered the breach.
    - Whether the non-public information was disclosed to/accessed by is an employee, vendor/contractor, or a member of the public.
    - The individuals affected by the breach.
- <u>Determining Severity of the Breach</u>:

- Whether the individual or entity that the data was disclosed to/accessed by will be able to retain the information.
- The type of data that was disclosed/accessed (ex. PHI or PII).
- Whether the data affected was destroyed, disclosed, manipulated, etc.
- Whether the data disclosed will undermine the security of other related data or will affect individuals not already affected.
- The number of individuals affected by the breach.
- The duration of the breach.
- Whether there continues to be access to non-public data.
- Whether the individuals affected are children, incapacitated, or especially vulnerable.
- How the affected individuals are likely to be affected by the breach. (Invasion of privacy? Reputation damage? Physical safety jeopardized?).

▪ Documentation:
- Whether the employee who caused the breach was authorized to access/manage the data that was disclosed.
- Whether the data was in electronic or physical form.
- Whether the breach occurred on the worksite or elsewhere.
- When the breach occurred.
- The cause of the breach.
- When the breach was discovered.
- How the breach was discovered.
- The security measures implemented prior to the breach.
- The mitigation activities conducted by the Department in response to the breach.
- When mitigation activities began.
- When notification to affected individuals was provided.
- Reasoning why notification to affected individuals was provided, or why it was not.

▪ Mitigation:
- When the Department began mitigation activities.
- How the Department is mitigating the breach.
- If the data is destroyed, whether the Department has a backup copy.
- If the data is manipulated, whether the Department is able to revert it back to its original state.

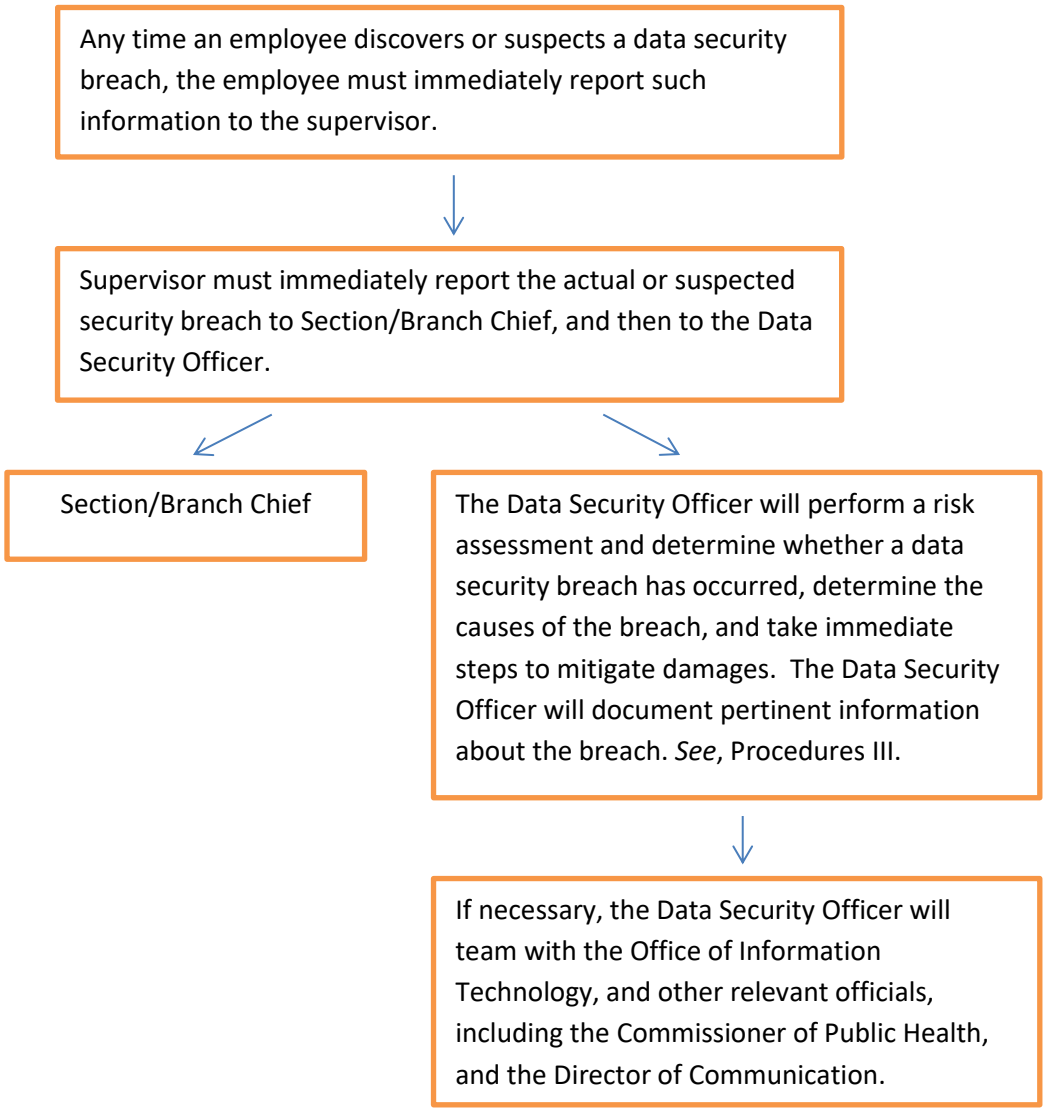
▪ Notification:
- The affected individuals who will receive notification of the breach.
- The type of notification that will be provided to affected individuals.
- When notification will be provided to affected individuals.
- Reasons for providing or not providing notification to affected individuals.

▪ Reporting:
- Fill out Form Report of Breach of Unsecured PHI or PII.
- Fill out Form Breach Resolution Form for the Commissioner's inspection and signature.

The Data Security Officer will team with the Office of Information Technology, and other relevant officials, including the Commissioner of Public Health, and the Director of Communication, when necessary.

The Data Security Officer along with other relevant officials such as manager will determine whether the affected individuals will be notified, and determine what additional steps will be taken to further mitigate damages.

PROCESS:



STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

REPORT OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION (PHI) OR PERSONALLY IDENTIFIABLE INFORMATION (PII)

(To be completed by DPH Manager or Business Associate)

Entity Reporting: _____ **Date**: _____

Date of Breach: _____ **Date of Discovery**: _____ **# of Persons Affected**: _____

Brief Description of the Incident:

_____

Actions taken to mitigate the harm of the breach or to prevent its recurrence:

_____

Breach Involved:

- **Email** ☐
- **Paper Records** ☐
- **Information Dissemination** ☐
- **Equipment** ☐

Type of Breach:

- **Compromise** ☐
- **Loss** ☐
- **Theft** ☐

Cause of Breach:

- **Failure to follow policy** ☐
- **Failure to safeguard information** ☐
- **Failure to safeguard equipment** ☐
- **Improper security settings** ☐
- **Other (explain in summary)** ☐

STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

Type of PHI or PII involved in the incident (Select all that apply):

☐	**Social Security Numbers**	☐	**Date of Birth**	☐	**Personal Phone Number**
☐	**Names**	☐	**PHI (health information) PII (Personal identifying information)**	☐	**Client or Medical Record Number**
☐	**Home Addresses**	☐	**Financial information (Specify)**	☐	**Other (Specify)**

If information was sent electronically was secure email or fax used? ☐ **Yes** ☐ **No**

Name of Person submitting this report:

Title/Organization:

Email: **Phone Number:**

Instructions for Completing this Form

General Information

The employee will contact his or her manager to report disclosures immediately after learning about the data breach. These improper disclosures may include incidents such as but not limited to:

- Sending unsecure email containing PHI or PII information

- Faxing information to the wrong person

- Mailing information to the wrong address

- Verbally providing information to an unauthorized person

- Accessing information for personal use

- Losing information in a public place

The manager will obtain as much factual information as possible about the details of the improper disclosure to complete this form.

Date of Breach: enter the date the breach occurred

Date Breach Discovered: enter the date the breach was initially discovered by an employee

Entity Reporting: Enter "DPH" or the name of the entity reporting

STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

DESCRIPTION OF THE INCIDENT:

Summarize the facts or circumstances of the theft, loss or compromise of PHI/PII or including:

- to whom and when was the disclosure made

- what was the content of the disclosure

- if it was a paper or electronic disclosure. If electronic information was sent, was it sent securely?

ACTIONS TAKEN IN RESPONSE TO THE BREACH:

- Summarize steps taken to mitigate actual or potential harm to the affected individuals and the organization. For example training, disciplinary action, policy modification, systems modification, retrieving the information promptly

- List findings form the investigation of the breach

- What steps were taken to have the improperly disclosed PHI/PII destroyed or returned to DPH

Breach Involved: Select from the list, Email, Info Dissemination, Paper Records or Equipment

Type of Breach: Select from the list, theft, loss or compromise

Cause of Breach: Select from the list, Failure to follow policy, Failure to Safeguard Equipment or Information, Improper Security settings, or other

Type of Personally Identifiable Information/ Personal Identifying information involved: select all that apply. If financial information is selected provide additional details in the summary.

STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

BREACH RESOLUTION

(For Privacy Officer or Legal Counsel)

Program Name:

Tracking #: **# of Individuals Affected**: **Date:**

Submitted By:

Summary of Incident:

Summary of Risk Assessment:

Notification Recommendation: ☐ **Notify Individuals Affected** ☐ **Do Not Notify Individuals Affected**

Justification:

Privacy Officer Signature _____

Commissioner: ☐ **Agrees** ☐ **Agrees in Part** **Disagrees**

Comments: (if disagree or agree in part)

Commissioner's Signature _____

STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

Policy Name:	Freedom of Information Requests	**Number:**	COMM-01-000
Procedure:	Page 2		
Applies to:	All DPH Sections, all DPH employees		
Position Responsible:	Director of Communications		
Effective Date:	06/07/2016	**Last Reviewed:**	06/07/2016
Approved:		**Date:**	06/14/16

PURPOSE:

The purpose of this policy and procedure at the Connecticut Department of Public Health (DPH) is to centralize the process of receiving, tracking and monitoring Freedom of Information (FOI) requests.

SCOPE:

This policy and procedure applies to all Connecticut DPH Sections and employees.

DEFINITIONS:

Routine FOI request: An FOI request that is typically seen by a program or employee. An FOI that can be easily responded to with minimal staff resources/time.

Non-routine FOI request: Any FOI request that deals with: DPH personnel or policies, gubernatorial/legislative matters, non-routine legal issues, or any other sensitive issue. This also includes requests that will require extensive staff resources/time to compile, requests potentially involving multiple agencies, requests that may require extensive redactions and/or assistance/advice from the DPH Legal Office, or requests that require language assistance.

POLICY:

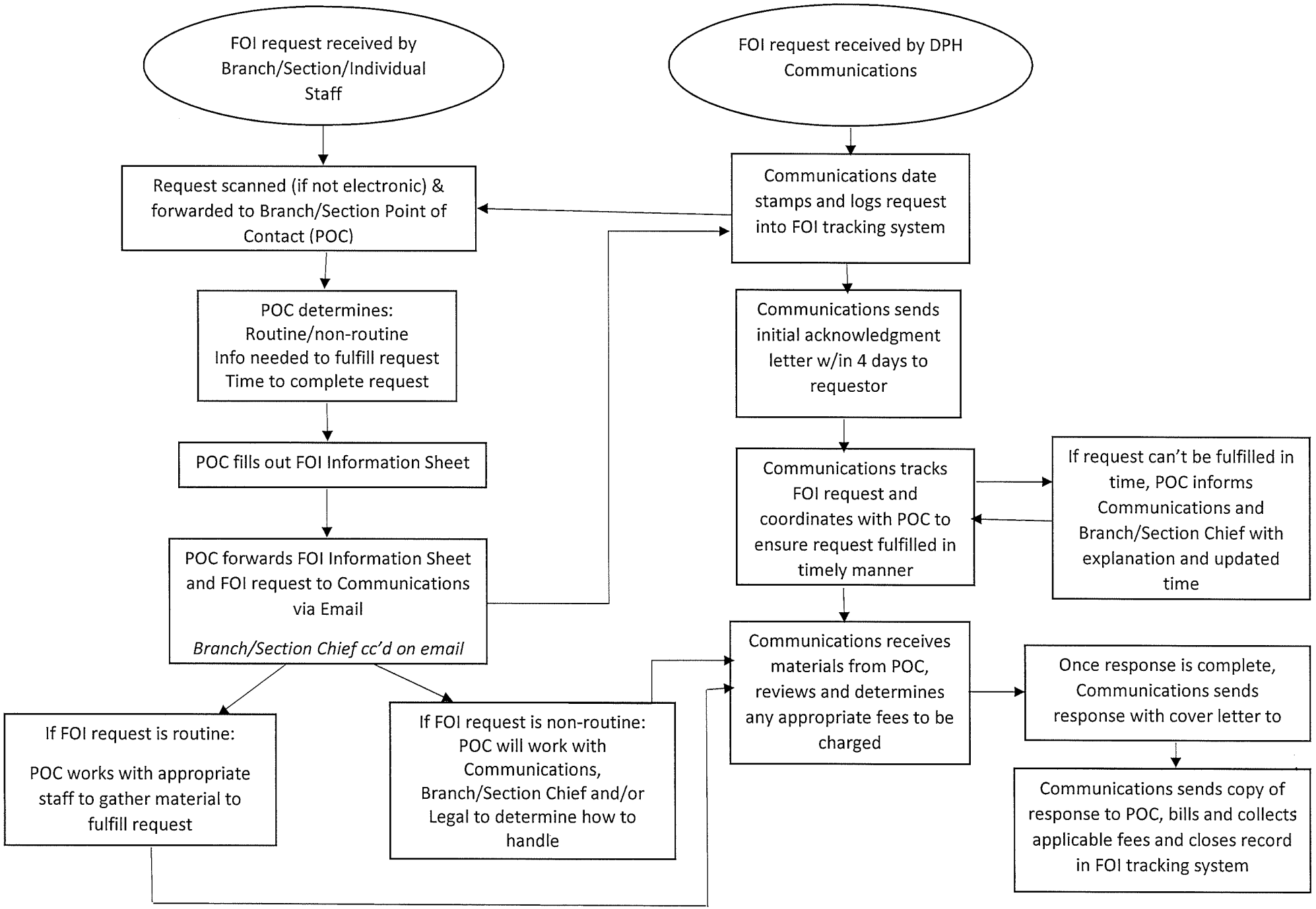
The Freedom of Information Requests policy at the DPH is to maintain a centralized repository for receiving, tracking and monitoring Freedom of Information requests which is essential for accountability and compliance with regulated requirements. DPH Communications (Communications) is the designated central processing section that will receive, track, monitor and disseminate FOI information.

PROCEDURES:

1. All DPH Branches and Sections will designate an FOI Point of Contact (POC) and forward the name of the contact person to the DPH, Communications Office. Points of Contacts are persons who will receive FOI requests and submit the FOI information to the DPH Communications Office. Each Branch/Section will also designate a back-up FOI Point of Contact who will be responsible for FOI requests when the primary POC is out of the office for more than one day.
2. The POC will read each FOI request he or she received from Communications or directly from a requestor and make a pre-determination as to whether it is a **routine** or a **non-routine** FOI request.
3. The POC will also determine an estimated time to complete the FOI request and provide an explanation for the estimate.
4. The POC will complete the DPH FOI Information Cover Sheet (see Appendix 1) and send it along with the FOI request to the Communications via, dph.communications@ct.gov. The POC will cc their Branch Chief and/or Section Supervisor on the email to Communications.
5. Except in cases where an FOI already has a receipt date, Communications will date stamp all FOI requests the day that they are received.
6. Communications will log or scan all FOI requests into a FOI tracking system and timely update the system to account for the processing of an FOI request from receipt to closing.
7. Communications will send the FOI requester a letter of acknowledgement within four (4) business days of receipt of the FOI and send a copy of it to the Point of Contact.
8. Communications will use the information provided in the FOI Information Cover Sheet to determine when to expect the requested information. The Letter of Acknowledgement will include an estimated delivery timeframe.
9. If the POC determines that a request cannot be fulfilled in the estimated time previously indicated, he or she will contact Communications via email, with a copy to either the Branch or Section Chief, with an explanation for the delay and an updated estimated time to complete the FOI request.
10. If subsequent conversations occur between the POC or Program and the requestor regarding changes to the scope of the FOI request, the POC will notify Communications via email. The email must include the date of subsequent conversation(s), with whom the conversation was held, and the substance of the changes to the FOI request. The email must include the original date of the FOI request and name of the requestor in the subject line for ease of identification.
11. Communications will also read each FOI request and confirm that the FOI is **routine** or **non-routine**.
12. Routine FOI requests will be prepared by the Program by the determined due date and be sent to Communications electronically, whenever possible, for distribution to the requester.

13. The DPH Legal Office will be available whenever there is a question or concern regarding any FOI request.
14. All **non-routine** requests require special handling, i.e., limiting the number of employees who handle the request, contacting the party involved to let him/her know about the request, requiring language assistance, redacting information as appropriate and having the party involved review the material prior to it being sent.
15. All **non-routine** request responses must be sent to Communications with a draft cover letter that explains all redactions and other changes from the original request.
16. Communications will disseminate the final response to the requester
17. Communications will maintain all information disseminated in a File Folder; separating **routine** and **non-routine** FOI requests and **redacted** and **non-redacted** FOI requests.
18. Communications will determine if any fees will be assessed, prepare an invoice to the requester, if appropriate, collect and process the fees through the DPH Fiscal Office
19. The DPH Fiscal Office will maintain accounts receivable records and process collections, if necessary

FOI Process Flow Chart



Template

Response to FOI request for STD, HIV, TB and Hepatitis Surveillance Data

Date

Dear XXXX:

Re: Your request under the Freedom of Information Act, dated July 17, 2019

Pursuant to the applicable law, based on the purpose of your request, the Department is unable to provide you with the information that you have requested.

Your request for information involves diseases that are reportable under Conn. Gen. Stat. §19a-215. A ''reportable disease'' is "a communicable disease, disease outbreak, or other condition of public health significance required to be reported to the department and local health directors." Conn. Agencies Regs. §19a-36-A1(dd).

"All information, records of interviews, written reports, statements, notes, memoranda or other data…" that DPH obtains in connection with a reportable disease is confidential and can only be used by DPH and local health directors for disease prevention and control and medical or scientific research. Conn. Gen. Stat. §19a-25. The terms "all" and "only" in the statute prohibit DPH from disclosing any information whatsoever unless the disclosure is for said research or disease prevention and control purposes. The corresponding regulations further clarify that the confidentiality requirement applies to information obtained from individuals and institutions and information about individuals and institutions. See Conn. Agencies Regs. §19a-25-1(6), (7), (11).

In light of these legal requirements, DPH cannot divulge the name of an institution, business, school, client, witness or any other information that it acquires during the course of an investigation of a reportable disease unless disclosure is required for disease prevention and control or medical or scientific research. In addition, when confidential information disclosure is permitted, DPH must limit the disclosure of identifiable health data to the minimum amount that is necessary to accomplish the public health purpose. Thus, if the Department has any documents containing information that is within the scope of the information that you seek through your request under the Freedom of Information Act for the purposes set forth in your request, the Department cannot disclose such information to you.

Sincerely,

APPENDIX 1

STATE OF CONNECTICUT
DEPARTMENT OF PUBLIC HEALTH

Raul Pino, M.D., M.P.H.
Commissioner

Dannel P. Malloy
Governor

Nancy Wyman
Lt. Governor

Office of Communications
Request for Freedom of Information (FOI)

Date Received:

Routine Request: ☐

Non-routine Request: ☐

Name of Office, Section, or Branch:

Contact Name: Contact Phone Number:

Requestor Name:

Company Name (if applicable):

Street Address:

Address (cont.):

City: State: Zip code:

Phone Number:

E-mail Address:

Anticipated Response Time:
(# of days, weeks, etc. & explanation)

Information Requested:

Date sent to Office of Communications:

Phone: (860) 509-8000 • Fax: (860) 509-7184
410 Capitol Avenue, P.O. Box 340308
Hartford, Connecticut 06134-0308
www.ct.gov/dph
Affirmative Action/Equal Opportunity Employer