

---

Legislative Program Review and Investigations Committee  
Connecticut General Assembly

---

Health Information Privacy in  
Selected State Programs

---

Staff Interim Update

October 1, 2015

**CONNECTICUT GENERAL ASSEMBLY  
LEGISLATIVE PROGRAM REVIEW AND INVESTIGATIONS COMMITTEE**

The Legislative Program Review and Investigations Committee (PRI) is a bipartisan statutory committee of the Connecticut General Assembly. Established in 1972, its purpose is to “conduct program reviews and investigations to assist the General Assembly in the proper discharge of its duties” (C.G.S. Sec. 2-53g). From program review topics selected by PRI, the committee examines “state government programs and their administration to ascertain whether such programs are effective, continue to serve their intended purposes, are conducted in an efficient and effective manner, or require modification or elimination” (C.G.S. Sec. 2-53d). Investigations require broader legislative approval to begin. The committee is authorized to raise and report bills on matters under its review.

The program review committee is composed of 12 members. The president pro tempore of the Senate, the Senate minority leader, the speaker of the House, and the House minority leader each appoint three members. The committee co-chairs and ranking members rotate every two years between House and Senate members from each party.

**2015-2016 Committee Members**

*Senate*

John W. Fonfara, *Co-Chair*

John A. Kissel  
Eric D. Coleman  
Anthony Guglielmo  
Joe Markley  
Andrew Maynard

*House*

Christie M. Carpino, *Co-Chair*

Mary M. Mushinsky  
Whit Betts  
Henry Genga  
Philip Miller  
Cara Pavalock

**Committee Staff on Project**

Scott Simoneau, Chief Analyst  
Michelle Castillo, Principal Analyst  
Alexis Warth, Legislative Analyst

---

Legislative Program Review and Investigations Committee  
Connecticut General Assembly  
State Capitol Room 506  
Hartford, CT 06106

# Interim Update Contents

---

## Health Information Privacy in Selected State Programs

This interim update report:

- identifies research questions intended to be answered by the study's conclusion, based on the study scope approved by the committee (Appendix A);
- explains the study timeline;
- discusses completed and anticipated PRI staff study activities; and
- presents selected background information relevant to understanding the study topic.

The next and final staff report following this interim report will:

- answer the identified research questions;
- make findings; and
- propose recommendations, if needed.

The final staff report will be presented after PRI staff has completed its research and analysis, which is ongoing. As noted in the study timeline, the final staff report is expected to be presented on or about December 16, 2015.

# Acronyms

---

AIDS	Acquired Immune Deficiency Syndrome
CDC	Centers for Disease Control and Prevention
CIRTS	Connecticut Immunization Registry and Tracking System
CPMRS	Connecticut Prescription Monitoring and Reporting System
CSA	Controlled Substances Act
CTEDSS	Connecticut Electronic Disease Surveillance System
DHHS	Department of Health and Human Services
EIP	Emerging Infectious Program
DAS/BEST	Department of Administrative Services/Bureau of Enterprise Systems and Technology
DCP	Department of Consumer Protection
DEA	Drug Enforcement Administration
DPH	Department of Public Health
FOIA	Freedom of Information Act
FOIC	Freedom of Information Commission
HAI	Health Acquired Infection
HIPAA	Health Insurance Portability and Accountability Act
HIV	Human Immunodeficiency Virus
IDS	Infectious Disease Section
PDA	Personal Data Act
PHI	Protected Health Information
PMP	Prescription Monitoring Program
STD	Sexually Transmitted Diseases

# Research Questions and Study Timeline

---

## Research Questions

1. What state and federal protections relate to health information privacy?
2. How are personal data being collected, accessed, shared, and safeguarded within Department of Public Health's (DPH) Infectious Diseases Section (IDS) and Department of Consumer Protection's (DCP) Prescription Monitoring Program (PMP)?
3. Do the health information management practices within these DPH and DCP programs meet the requirements of state and federal laws?

## Study Timeline

- **July 9, 2015:** PRI voted to approve a study scope.
- **October 1, 2015:** PRI staff is scheduled to present this interim study update to the committee.
  - After the interim study update on the same day, PRI will hold an informational public hearing to gather input and viewpoints relevant to the study topic directly from interested parties.
- **On or about December 16, 2015:** PRI staff will present its final report containing background, findings, and recommendations to the PRI committee for its consideration of and action on recommendations.
- **After December 16, 2015:** The final committee-approved study report will be published.
- **During the 2016 legislative session:** The PRI committee may raise legislation for the 2016 legislative session to implement any study recommendations through statute. Any bills raised by PRI based on study recommendations would be the subject of a public hearing during the 2016 legislative session.

## Completed

1. Interviews with executive branch agencies
  - Department of Consumer Protection
    - Division of Drug Control
      - Prescription Monitoring Program
  - Department of Public Health
    - Various programs within the Infectious Diseases Section
2. Interviews with stakeholders
  - American Civil Liberties Union
  - Connecticut Medical Society
  - Connecticut Police Chiefs Association
  - Connecticut Association for Directors of Health
3. Requested data or reports from various organizations
  - Department of Consumer Protection
  - Department of Public Health
4. Other background/expert interviews
  - National Conference of State Legislatures
  - Director of Information Technology, Connecticut General Assembly

## Anticipated

1. Additional interviews with executive agency personnel and stakeholders
2. Development of database inventory
3. Analysis of the type of personal health information data collected
4. Analysis of how information is collected, stored, shared, and safeguarded
5. Evaluation of third-party safeguards
6. Evaluation of interagency and intergovernmental agreements

## Topic Background

---

Health information has been subject to heightened concerns about confidentiality as many core public health activities rely on the acquisition, storage, and use of personal information. As noted in the committee's approved scope, this study is evaluating the management of personal health information, including compliance with certain confidentiality requirements, at the Department of Public Health's (DPH) Infectious Disease Section (IDS) and the Department of Consumer Protection's (DCP) Prescription Monitoring Program (PMP).

This report provides a general summary of the major federal and state laws addressing health information privacy and their applicability to the selected programs under PRI study. This report also provides a basic profile of each of the selected programs including its purpose, organization, mandated reporters, reportable items, and an overview of each program's generalized data flow. This document does not contain detailed analysis, findings, or recommendations, which will be included in the December report.

### What State and Federal Laws Relate to Health Information Privacy?

As explained below, the IDS and PMP programs are primarily subject to department and program specific information privacy laws and regulations, due to a variety of exemptions found in the overarching federal and state privacy laws. When discussing the role of government in the handling of personal information, there are three primary considerations that drive the policymaking process: a need for transparency, a need to protect individual privacy, and programmatic needs for shared information. The desire to balance these considerations can be seen within many of the state and federal statutes and policies that address the handling of personal information.

For the purpose of this report, statutes and regulations addressing information privacy and security are divided into: (1) umbrella laws: the federal Health Insurance Portability and Accountability Act (HIPAA), the state Freedom of Information Act (FOIA), and the state Personal Data Act (PDA)<sup>1</sup>; and (2) department specific laws and regulations for DPH and DCP. (A summary of each law can be found in Table 1, with further descriptions in Appendices B through E.)

**Health Insurance Portability and Accountability Act.** HIPAA is a federal law adopted in 1996 in an effort to ensure that individuals could retain health insurance coverage after leaving an employer and to provide standards to protect the privacy and security of healthcare data. HIPAA established a "national minimum of basic protections" for individual privacy, while still allowing for necessary data collection and sharing. HIPAA regulations only apply to "covered entities," which are defined as health plans, healthcare clearinghouses, and healthcare providers.<sup>2</sup>

---

<sup>1</sup> Additional federal laws concerning privacy, such as the federal Privacy Act and the federal Freedom of Information Act, only apply to federal agencies.

<sup>2</sup> 45 C.F.R. §160.103.

*Applicability to IDS and PMP.* As government programs, IDS and PMP are not subject to HIPAA requirements, due to the fact that neither program falls into any of the three covered entity categories. However, covered entities are able to share protected health information with DPH and DCP due to the public health provisions within HIPAA,<sup>3</sup> as well as Connecticut state law that mandates reporting practices.

**Freedom of Information Act.** The Freedom of Information Act (FOIA) is a Connecticut state law passed in 1975, which “provides the public with rights of access to records and meetings of public agencies.” The primary intent of FOIA is to increase transparency and accountability of government entities.<sup>4</sup> Under FOIA, members of the public are able to request access or copies of records maintained by public agencies, as well as the opportunity to attend public agency meetings.<sup>5</sup> If a public record is already subject to specific access rules or restrictions under state or federal statute, the record is not subject to FOIA release requirements.

*Applicability to IDS and PMP.* Records collected and maintained by IDS and PMP are generally considered outside of, or excluded from, FOIA requests. FOIA excludes medical and personnel files, as well as any records pertaining to an ongoing public health investigation.<sup>6</sup> In addition to the exclusions outlined in FOIA, records collected and maintained by IDS and PMP are classified as confidential within Connecticut statutes.<sup>7</sup>

**Personal Data Act.** The Connecticut Personal Data Act was passed in 1976 to establish responsibilities and standards for data collection, usage, and storage within state and municipal agencies. The act includes responsibilities and standards, such as staff training, reasonable precautions for the protection of personal data, and procedures to ensure individuals’ access to their own personal data.<sup>8</sup>

*Applicability to IDS and PMP.* IDS and PMP are exempt from the information sharing requirements in the Personal Data Act, due to the statutory confidentiality of their program records. While these programs are not required to make their records available to individuals, IDS and PMP are still mandated to follow the other standards within PDA, including employee training on privacy laws, reasonable efforts to protect data, and the adoption of regulations describing what information is collected and how it is handled.<sup>9</sup>

**Department and program specific laws and regulations.** While IDS and PMP are exempt from many of the data handling requirements outlined in the laws discussed above, each

---

<sup>3</sup> 45 C.F.R. §164.512(a) and §164.512(b). In addition to these two sections, HIPAA also includes specific scenarios where state law preempts HIPAA, including the regulation of controlled substances and public health surveillance, investigation and intervention (45 C.F.R. §160.203). These preemptions allow state law to require covered entities to release protected information to DCP and DPH.

<sup>4</sup> FOIC, *Citizen’s Guide*, (2008, Rev. 2011). Accessible at <http://www.ct.gov/foi/cwp/view.asp?a=4161&q=488530>

<sup>5</sup> Appendix D provides more background information about FOIA.

<sup>6</sup> C.G.S. Sec. 1-210(b)(2) and C.G.S. Sec. 1-210(b)(16).

<sup>7</sup> C.G.S. Sec. 19a-25 and C.G.S. Sec. 20-578.

<sup>8</sup> See Appendix E for further description of PDA.

<sup>9</sup> C.G.S. Sec. 4-193 and C.G.S. Sec. 4-196.

department must comply with agency and program specific state statutes and regulations concerning the collection, maintenance, and use of personal data. These citations can be found in Appendix B. Of particular importance are citations that establish the confidentiality of IDS and PMP program records.

*Department of Public Health.* All information collected, maintained, or used by DPH for the purpose of studying and/or reducing morbidity and mortality from any cause or condition is required to be confidential pursuant to state law.<sup>10</sup> Statutory language specifically establishes confidentiality for information within the reportable disease program.<sup>11</sup> The usage and release of health data is at the discretion of DPH for three primary purposes: research, enforcement, and, when necessary, protection of health, life, or well-being.<sup>12</sup> In all three scenarios, DPH is required to make every effort to “limit the disclosure of identifiable health data to the minimal amount necessary to accomplish the public health purpose.”<sup>13</sup>

*Department of Consumer Protection.* The information collected by DCP through filed reports, inspection, or as otherwise authorized “shall not be disclosed publicly in such a manner as to identify individuals or institutions.”<sup>14</sup> Additional statutory language establishes confidentiality specifically for records collected through PMP.<sup>15</sup> DCP may provide prescription information obtained from pharmacies through PMP for the following purposes: regulatory, investigative, or law enforcement purposes; patient care and drug therapy management by practitioners and pharmacists; and statistical, research, or educational purposes.<sup>16</sup> When used for research purposes, DCP is required to ensure that the “privacy of patients and confidentiality of patient information is not compromised.”<sup>15</sup>

Additional state statutes and regulations outlining the collection, usage, and protection of personal information within DPH and DCP may be found in Appendix B.

---

<sup>10</sup> C.G.S. Sec. 19a-25.

<sup>11</sup> C.G.S. Sec. 19a-25.

<sup>12</sup> Conn. Agency Regs. Secs. 19a-25-1 to 19a-25-4.

<sup>13</sup> Conn. Agency Regs. Sec. 19a-25-3.

<sup>14</sup> C.G.S. Sec. 20-578.

<sup>15</sup> C.G.S. Sec. 20-578.

<sup>16</sup> Conn. Agency Regs. Sec. 21a-254-6.

**Table 1: Major Laws Concerning Data Privacy**

Law	Summary	Who is covered?	Applies to IDS?	Applies to PMP?
<p><b>Health Insurance Portability and Accountability Act (HIPAA)</b></p> <p>Public Law 104-191 45 C.F.R. §§160—164</p>	<p>Passed by Congress in 1996, HIPAA was adopted to ensure health insurance coverage after leaving an employer and to provide national minimum standards for the privacy and security of protected health information.</p>	<p>The relevant sections of HIPAA for this report (Privacy Rule and Security Rule) apply to covered entities, which are defined as health plans, healthcare clearinghouses, and healthcare providers.</p>	<p><b>No.</b> IDS is not considered a covered entity, so is exempt from HIPAA requirements.</p>	<p><b>No.</b> DCP is exempt from HIPAA requirements due to the fact that it is not a covered entity.</p>
<p><b>Freedom of Information Act (FOIA)</b></p> <p>C.G.S. Secs. 1-200 to 1-242</p>	<p>Passed by the Connecticut General Assembly in 1975, FOIA affords individuals the right to access records and attend meetings held by public agencies. The goal of FOIA is to increase transparency among public agencies.</p>	<p>All executive, administrative, and legislative offices in Connecticut, including any political subdivisions of the state or towns (such as school districts).</p>	<p><b>No.</b> Records collected and/or maintained by IDS are exempt from FOIA requirements due to exemptions within FOIA and the statutory authorization of DPH. DPH is still required to respond to FOIA requests within a prompt period of time.</p>	<p><b>No.</b> Information contained in the state PMP system is exempt from FOIA requirements due to exemptions within FOIA and the statutory authorization of DCP and PMP. DCP is still required to respond to FOIA requests within a prompt period of time.</p>
<p><b>Personal Data Act (PDA)</b></p> <p>C.G.S. Secs. 4-190 to 4-197</p>	<p>The Personal Data Act was passed in 1976 with the intent of establishing responsibilities and standards for data collection, usage, and storage within state and municipal agencies. The act also affords individuals the right to request information on what personal data is being collected/shared by each agency.</p>	<p>All state or municipal boards, commissions, departments, or officers. The legislature, courts, Governor, Lieutenant Governor, Attorney General, and town/regional boards of education are exempt.</p>	<p><b>Partially.</b> IDS is exempt from the data sharing portions of the PDA, due to the confidentiality written into the statutory authorization of DPH. IDS is still responsible for adhering to the training and data handling requirements in PDA.</p>	<p><b>Partially.</b> PMP is exempt from the data sharing portions of the PDA, due to the confidentiality written into the statutory authorization of DCP and PMP. PMP is still responsible for adhering to the training and data handling requirements in PDA.</p>

Source: PRI

## How Is Personal Information Defined?

The definition of personal information varies depending on context and source. Definitions of personal information from relevant federal and state laws are described below. Variations that exist between definitions can broaden or narrow the scope of information that is considered personally identifying and, therefore, subject to privacy protections.

An important consistency found among many definitions of personal information is the concept that individual variables, as well as combinations of variables, can be considered identifying. In most contexts, it is the responsibility of the party maintaining the data to determine what combination of information could be potentially identifying. (A further discussion and analysis of these definitions will be found in the December report.)

**Health Insurance Portability and Accountability Act.** The definition included in HIPAA is for protected health information, which includes a list of 18 identifiers of a person, or of relatives, employers, or household members of a person, that must be removed before information is considered de-identified. These identifiers include names, all geographic subdivisions smaller than a state, age/date of birth, Social Security numbers, and biometric identifiers.<sup>17</sup>

**Personal Data Act.** Personal data is defined in the Connecticut Personal Data Act as “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.”<sup>18</sup>

**Freedom of Information Act.** The Connecticut Freedom of Information Act does not contain a specific definition of personal information or personal data. FOIA provides access to “public records or files,” which are defined as “any recorded data or information...prepared, owned, used, received or retained by a public agency.”<sup>19</sup> This broad definition is limited by a number of exclusions, including certain information that could be considered personal data, such as medical or personnel records.<sup>20</sup>

## What do DPH and DCP Consider Personal Information?

A description of the personal information that is collected by IDS and PMP can be found in the following statutes and regulations:

*Department of Public Health.* The personal data collected/maintained for reportable disease purposes include, but are not necessarily limited to: “name, address, age, race/ethnicity, sex, occupation, and behaviors which put the individual at risk for infectious disease.”<sup>21</sup>

---

<sup>17</sup> Full list of identifiers can be found in Appendix C. Source: 45 C.F.R. §164.514(b)(2)(i).

<sup>18</sup> C.G.S. Sec. 4-190(9).

<sup>19</sup> C.G.S. Sec. 1-200(5).

<sup>20</sup> Full list of exclusions can be found in C.G.S. Sec. 1-210.

<sup>21</sup> Conn. Agency Regs. Sec.19a-2a-12(b)(1) and Conn. Agency Regs. Sec. 19a-36-A4.

Identifiable health data is defined as “any item, collection, or grouping of health data that makes the individual or organization supplying it, or described in it, identifiable.”<sup>22</sup>

*Department of Consumer Protection.* Prescribing physicians are required to submit the following information to PMP: date of receipt, the name and address of the person who received the prescription, and the kind and quantity of controlled substances received.<sup>23</sup> Pharmacies are required to submit the following information to PMP: prescription information (such as number, dose, and DEA number), patient identification number, patient’s first and last name, patient’s street address, patient’s date of birth, and the type of payment used.<sup>24</sup>

### **What Is the Minimum Necessary Information Requirement?**

There is language in both HIPAA and PDA requiring that any entity gathering, maintaining, or utilizing protected personal information should use or disclose only the minimum information necessary to complete a specific task.<sup>25</sup> The PDA states that “each agency shall maintain<sup>26</sup> only that information about a person which is relevant and necessary to accomplish the lawful purposes of the agency.”<sup>27</sup> The federal Department of Health and Human Services describes the minimum necessary requirement as a “key protection” within the Privacy Rule of HIPAA. While the departments discussed in this report are not covered entities under HIPAA, the emphasis on the minimum necessary requirement demonstrates the importance of this concept within any health privacy discussion.<sup>28,29</sup>

### **DPH’s Infectious Diseases Section**

The next area of this interim report provides background information on the Department of Public Health’s (DPH) Infectious Diseases Section (IDS). This includes a description of IDS’ responsibilities, how the section is organized, reportable diseases, mandated reporters, and a general overview of how reportable disease information flows through IDS.

### **What Is the Purpose of DPH’s Infectious Diseases Section?**

The Connecticut Department of Public Health is the lead agency in the effort to protect the public’s health, including the provision of health information, policy, and advocacy efforts. Specific DPH activities include oversight of local health departments, adopting and enforcing

---

<sup>22</sup> Conn. Agency Regs. Sec.19a-25-1(7).

<sup>23</sup> C.G.S. Sec. 21a-254(f).

<sup>24</sup> C.G.S. Sec. 21a-254(j)(3).

<sup>25</sup> DHHS, *Guidance: Significant Aspects of the Privacy Rule*, available at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coverentities/minimumnecessary.html>

<sup>26</sup> In the Personal Data Act, the term *maintain* is defined as collect, maintain, use or disseminate (C.G.S. Sec. 4-190(6)).

<sup>27</sup> C.G.S. Sec. 4-193(e).

<sup>28</sup> The minimum necessary requirement is considered “central” to the Privacy Rule section of HIPAA, with specific descriptions being found in 45 C.F.R. §164.502(b) and 45 C.F.R. §164.514(d).

<sup>29</sup> DHHS, *Guidance: Significant Aspects of the Privacy Rule*, available at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coverentities/minimumnecessary.html>.

health regulations and rules, educating communities, providing grant funding and contracts for direct-service programming, and tracking and responding to health epidemics.

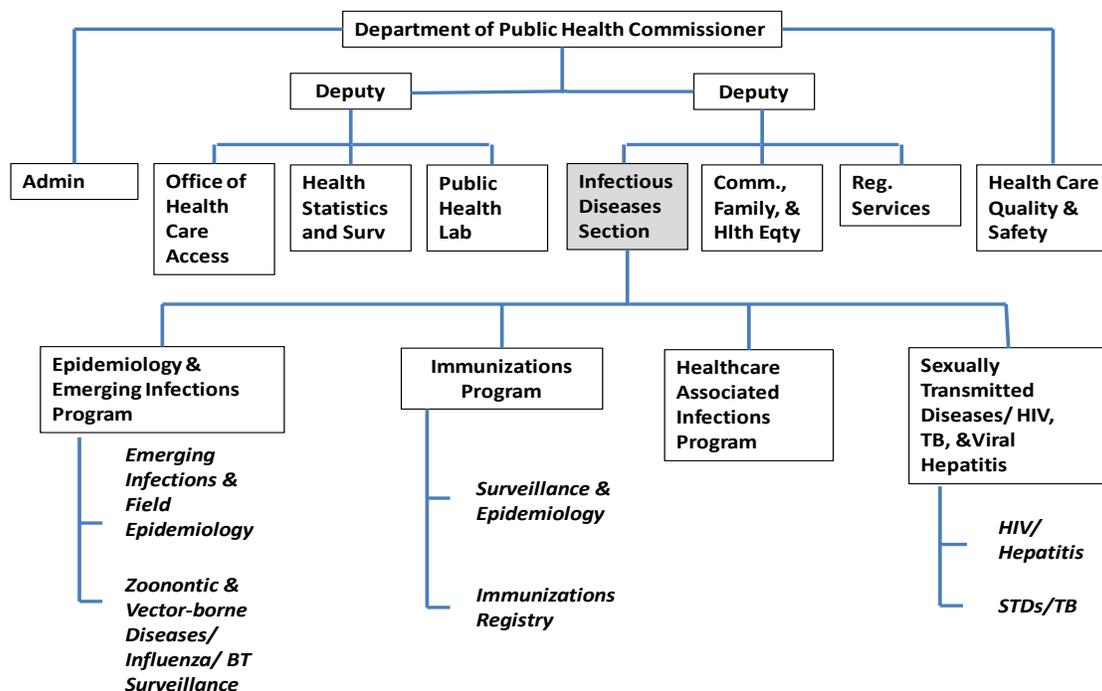
The Infectious Diseases Section is responsible for:

- collecting data from across the state to assess infectious diseases and associated risk factors;
- identifying and responding to emerging infections; and
- conducting outbreak investigations and surveillance.<sup>30</sup>

### How Is the Infectious Diseases Section Organized?

The Infectious Diseases Section is one of eight subdivisions of DPH as shown below. The section is further divided into four broad programs with about 100 employees. The six units below the programs are areas that collect personally identifiable health information.

**Figure 1. Department of Public Health’s Infectious Disease Section Organization**



Source: DPH

<sup>30</sup> “Public health surveillance is the systematic, ongoing collection, management, analysis, and interpretation of data followed by the dissemination of these data to public health programs to stimulate public health action.” Porta M, ed. Dictionary of Epidemiology. 5th ed. International Epidemiological Association. New York, NY: Oxford University Press; 2008. Cited in: Centers for Disease Control and Prevention. *CDC’s Vision for Public Health Surveillance in the 21<sup>st</sup> Century*. MMWR 2012;61(Suppl; July 27, 2012): p 3.

**Epidemiology and Emerging Infections Program** - This program:

- conducts surveillance for more than 30 infectious diseases;
- investigates disease outbreaks;
- conducts epidemiologic studies of emerging infectious diseases; and
- provides training and creates public education programs to develop, evaluate, and promote prevention and control strategies for infectious diseases.

**Immunizations Program** – The program’s purpose is to prevent disease, disability, and death from vaccine-preventable diseases in infants, children, adolescents, and adults through:

- surveillance;
- case investigation and control;
- monitoring of immunization levels;
- provision of vaccines; and
- professional and public education.

This program administers the Connecticut Immunization Registry and Tracking System (CIRTS), which is a statewide database that includes information to assess the current immunization status of children.

**Healthcare Associated Infections (HAI) Program** - This program focuses on surveillance of HAIs and the dissemination of best practices for prevention. The scope of the HAI program includes a variety of infection types that are:

- associated with healthcare procedures and devices (e.g., infections associated with central lines and surgical procedures);
- transmitted in healthcare facilities (e.g., *Clostridium difficile*, influenza); and
- antimicrobial resistant micro-organisms.

**Sexually Transmitted Diseases (STD) Control Program** - This program aims to reduce the occurrence of STDs through:

- disease surveillance;
- case and outbreak investigation;
- screening and preventive therapy;
- outreach and diagnosis;
- case management, and
- education.

The Department of Public Health mandates reporting of five STDs: syphilis, gonorrhea, chlamydia, neonatal herpes, and chancroid. In addition, HIV/AIDS, hepatitis, and tuberculosis surveillance, case investigation, and outreach are conducted by this program.

### **What Are the Reportable Diseases?**

The DPH commissioner is required by statute to update and publish on an annual basis a list of diseases and laboratory findings that certain healthcare providers and others (described below) must report to the department and the local health director of the town in which the patient resides (i.e., reportable diseases). The department relies on an advisory committee, consisting of public health officials, clinicians, and laboratorians, to assist with the annual list revision; it also receives guidance from federal sources. For calendar year 2015, there were two additions and one modification to the healthcare provider list of reportable diseases, and one addition, one removal, and six modifications to the laboratory list of reportable diseases.

Currently, there are over 80 reportable diseases that are classified by DPH into two categories. Category 1 diseases, such as tuberculosis, measles, and foodborne outbreaks must be immediately reported by telephone on the day the disease is recognized or strongly suspected and a written report must be mailed or faxed to DPH within 12 hours. Category 1 diseases require an immediate public health response and include possible bio-terrorism agents.

Category 2 diseases, such as Hepatitis C, human immunodeficiency virus (HIV), or influenza-associated deaths, do not require telephone reporting but must be reported within 12 hours of recognition or strong suspicion of the disease by completing the appropriate report form and mailing or faxing it to DPH. (A full list of the reportable diseases can be found in Appendix F).

### **What Is the Minimum Information Typically Reported?**

Most reportable diseases are reported through a standard form created by DPH. Some diseases require that supplemental forms be filled out or in a few cases a different specialty form entirely.<sup>31</sup> Nonetheless, each report includes the following minimum information:

- full name, address, date of birth, race/ethnicity, age, sex, and occupation of person affected;

---

<sup>31</sup> Specialty forms are used for reporting cases of HIV/AIDS, Influenza, Sexually Transmitted Diseases, Tuberculosis, and Varicella.

- diagnosis or suspected disease;
- date of onset of illness;
- the lab results, risk factors, and symptoms for certain diseases;
- full name, address, and telephone number of the attending physician; and
- full name, address, and telephone number of the person reporting as well as the date of the report.

Some specialty forms used to conduct follow-up interviews may include additional personal information, such as the identification of other people with whom the affected person has had contact and the place of business at which the affected person works. The December report will provide additional analysis of this information.

### Who Are the Mandated Reporters for Infectious Diseases?

There are three categories of individuals who are required to notify DPH and the patient’s local health department regarding a case or suspected case of reportable disease as illustrated in Table 2 below. Most reports come from physicians and clinical laboratories.

**Table 2: Persons Required to Report Reportable Diseases**

Category	Examples
<b>Health Care Providers</b>	Licensed physicians Nurse practitioners Physician assistants Nurses Dentists Medical examiners
<b>Health Care Facilities (person in charge)</b>	Hospitals Long-term care facilities Clinics State facilities caring for persons with developmental disabilities, mental illness, or substance abuse
<b>Other</b>	School/day care administrators Camp director Ship captain/Master Aircraft pilot/Master Person in charge of a dairy processor/ Food processor or sales/ Non-alcoholic beverage sales or distributor Morticians/Funeral directors

Source: Conn. Agency Regs Sec. 19a-36-A3.

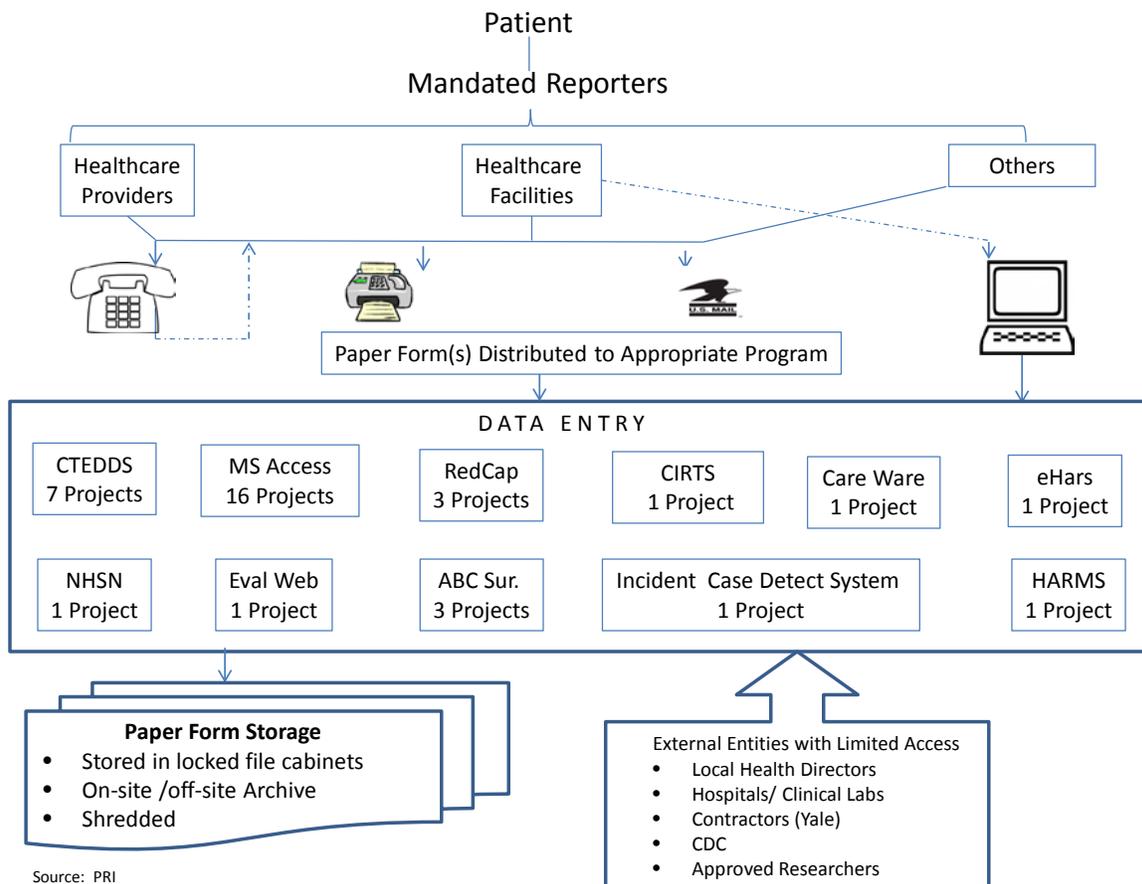
Further, the director of a clinical laboratory must report any laboratory results that are suggestive of a reportable disease. This report is in addition to the report a health care provider must also fill out. The lab report, in most cases, allows for verification of the diagnosis. The state also has a public health laboratory that provides testing for bacterial, viral, and parasitic agents of diseases and serves as a reference center for microbiological aspects of infectious diseases, meaning that it has a greater capability to fully identify disease agents of public health importance.

### How is Information Received, Stored, and Accessed within IDS?

Figure 2 illustrates how infectious disease health information typically flows through IDS. The figure depicts this flow in a very general way and does not include a description of safeguards or follow-up investigatory activities (which will be a subject discussed in the December report).

Typically, IDS organizes its work by projects within program areas. There are a number of steps and variations that occur within individual projects that have not been included in order to provide an overall sense of the main stages of the process. The key points in the process are highlighted below.

**Figure 2. Reportable Disease Information Flow**



1. **Collection of information.** The mandated reporters typically fill out common forms (P-23 for providers; OL15-C for laboratories) for most reportable diseases. Some diseases require additional or disease-specific forms. The Infectious Diseases Section is also involved in research projects that only involve specific cases, type of diseases, or areas of the state, and these data collection sheets will vary from the common form. After the necessary information is collected by the mandated reporter, it must be submitted to DPH.
2. **Mode of transmission.** There are four primary modes through which DPH will receive reportable disease information: telephone, facsimile, U.S. mail, and electronically. Electronic reporting is done either by accessing a data system via secure web-based data entry or by the uploading of electronic files. As noted above, certain diseases require an immediate response and must be phoned into DPH. Even in those cases, certain forms must also be filled out and submitted either through a paper form or electronically. DPH will also give guidance over the phone to the mandated reporters who call regarding patient care and remind them to fill out the appropriate form.

Most of the completed forms are received through the mail or by facsimile. Forms that are mailed must be marked “confidential.” In no case is email used to transmit personally identifiable health information. In addition, certain healthcare providers have access to certain web-enabled databases for the purpose of data entry. For example, all pediatricians are required to report the immunization status of children under their care into CIRTS and some do this via web-entry. A few reporters, such as hospitals and local health departments, have web-enabled access to the Connecticut Electronic Disease Surveillance Systems (CTEDSS) for data entry of certain diseases.

3. **Data entry.** The information, including personal health data, contained on the forms is entered into one of 28 databases by DPH personnel, their designees, or entered directly by certain facilities and practitioners. The size of the databases range from fairly small Microsoft Access databases with hundreds of records to the very large proprietary CTEDSS that has thousands of records. Some of the same information is entered into more than one database. Many of the small databases involve various research projects that are sponsored by the U.S. Centers for Disease Control and Prevention (CDC). Many database servers are located at DPH, others are located within the Department of Administrative Services’ Bureau of Enterprise Systems and Technology (DAS/BEST), while others are located with the CDC and in one case with the City of Hartford. Appendix G contains a list of databases and indicates the diseases that are tracked, the type of information technology platform on which the database resides, name of the creator of the database, location of the database, and if there is remote access to the database. The listing also indicates the primary reason for the data being collected which is usually either disease surveillance or research. Most of what IDS does is surveillance which is an on-going and systematic effort of data

collection and interpretation that often leads to some public health response. Some of that information may be used for research which may or may not result in actions being taken by IDS but usually adds new knowledge about a particular disease.

4. **Paper form storage.** Thousands of paper forms are generated through this reporting process. The department adheres to the Connecticut State Library Office of Public Records Administrator's record retention schedule. In general, forms are kept for one year in locked file cabinets in the office space of the program that oversees the particular disease area or research project. Forms may then be archived either on-site or off-site. Archived files are kept for at least three years, after which the documents are shredded. The retention practice can vary widely. For diseases with a fairly low volume of reports, for example, program managers may decide to keep several years of forms in a locked file cabinet.
5. **Access to information.** Various IDS staff have differing levels of access to databases depending on their role. Certain staff may only have access to disease specific databases whereas DPH managers may have broader access to a variety of databases. A number of outside organizations also have limited access to infectious disease information. For example, local health departments have access to infectious disease information in CTEDSS about residents of their jurisdiction. Similarly, hospitals have access to infectious disease information about their own patients contained in CTEDSS database. Pediatric providers have access to their patient's immunization status. Yale University is a contractor that partners with DPH in conducting various studies of infectious diseases and, therefore, has specific access to relevant data. The CDC receives de-identified data from DPH to track the occurrence of certain diseases. Finally, other researchers can request access to infectious disease data but must go through a rigorous review process. The department's Human Investigations Committee is charged with reviewing, monitoring, and approving investigative research that may include identifiable health data obtained by the department.

It should be noted that initial reports of certain contagious diseases may trigger the need for additional investigation by the department and the collection of supplementary personal health information. For example, the reporting of tuberculosis requires an interview of the patient within three days to determine who came into contact with the infected person and determine levels of exposure. Similar investigations are conducted for certain sexually transmitted diseases. There are also cases where the documented follow-up activities include a local health department monitoring a patient and verifying the patient takes his/her medication.

### **Facts and Statistics for Infectious Diseases Section**

- Connecticut is one of the few states that require reporters to file reports with both the local health department and the state.
- Over 24,000 cases of reportable diseases were reported in 2014 in Connecticut. (See Appendix H for a 2014 listing of reports of reportable disease)

- The highest number of reportable disease cases in 2014 included:
  - Chlamydia (12,732);
  - Hepatitis C (2,410); and
  - Lyme disease (1,675).

## **DCP's Prescription Monitoring Program (PMP)**

The Prescription Monitoring Program (PMP) maintains a statewide electronic database of dispensed prescriptions for controlled substances. The program also conducts community and professional outreach and education on prescription drug abuse, safe storage and disposal of prescription medication, and proper medication use.

### **What Is the Purpose of the Prescription Monitoring Program?**

Established in 2008, the purpose of the PMP is to assist authorized physicians and pharmacists in providing better informed treatment to their patients and to prevent the improper or illegal use of controlled substance prescription drugs. (See Appendix I for list of controlled substances.)

The PMP's central database, known as the Connecticut Prescription Monitoring and Reporting System (CPMRS), gives registered users a complete picture of a patient's controlled substance use, including prescription history from other providers. The information may aid health care providers in identifying patterns of prescribing, dispensing, or receiving controlled substances that may indicate abuse, misuse, or potential adverse drug interactions. This allows the prescriber to properly manage a patient's treatment, which may include referral to services for drug abuse or addiction, if appropriate.

### **How is the Prescription Monitoring Program Organized?**

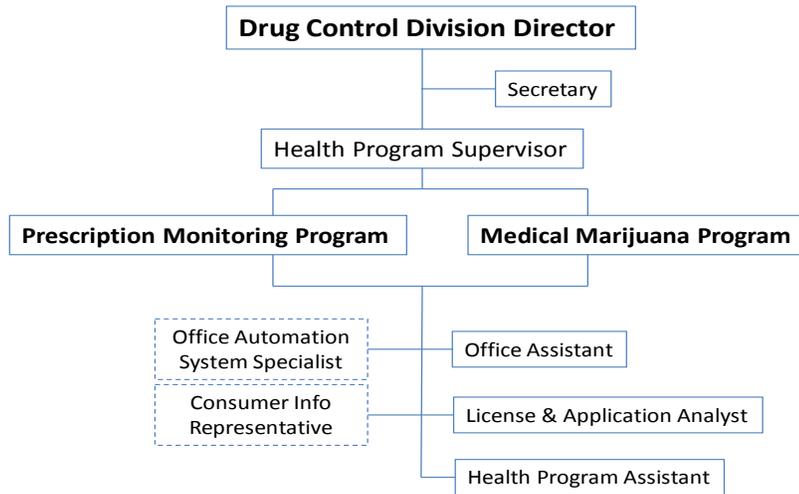
Organizationally, the PMP is housed within the Drug Control Division in the Department of Consumer Protection (DCP). The division regulates all entities involved in the distribution of legal drugs, medical devices, and cosmetics in the state. It also oversees licensure of pharmacies, pharmacists, controlled substance providers and laboratories, pharmacy technicians, and drug manufacturers and wholesalers. As such, the division is responsible for four major areas: compliance and enforcement; assisting the state Pharmacy Commission; and operating the PMP and the Medical Marijuana Program.

As seen in Figure 3, the PMP is administratively linked with the Medical Marijuana Program, which handles the application process for the registration certificate of patients who are currently receiving medical marijuana treatment for a debilitating condition. Both programs are managed by a health program supervisor and headed by a division director. In addition to the program supervisor, the PMP has an office automation system specialist for information technology issues.

The division also has a licensing and application analyst, a health program assistant, and a consumer information representative for the medical marijuana program. Staff for the

marijuana program, except for the consumer representative, has access to the PMP database to check if distributors are registered. (The Drug Control Division also has 12 drug control agents to deal with regulatory compliance and enforcement, which are not part of this study scope.)

**Figure 3. Department of Consumer Protection Drug Control Division**



Source: DCP (July 2015)

### Who Are the Mandated Reporters for PMP?

Pursuant to state law, all prescribers in possession of a Connecticut Controlled Substance Registration issued by DCP are required to register as a user with the CPMRS.

Any prescribing practitioner who is licensed by the state of Connecticut and dispenses controlled substances from their practice or facility is required to upload dispensing information into the CPMRS database. By statutory definition a “practitioner” refers to:

- “a physician, dentist, veterinarian, podiatrist, scientific investigator or other person licensed, registered or otherwise permitted to distribute, dispense, conduct research with respect to or to administer a controlled substance in the course of professional practice or research in this state; or
- a pharmacy, hospital or other institution licensed, registered or otherwise permitted to distribute, dispense, conduct research with respect to or to administer a controlled substance in the course of professional practice or research in this state.”<sup>32</sup>

<sup>32</sup> C.G.S. Sec. 21a-240.

However, a hospital pharmacy, long-term care facility pharmacy, or correctional facility pharmacy must report information for outpatients only. The controlled substance reporting requirements also do not apply to any institutional pharmacy or pharmacist's drug room operated by a facility that directly dispenses or administers to patients an opioid agonist for treatment of a substance use disorder (e.g., methadone clinic).

Other mandated reporters include nonresident pharmacies<sup>33</sup> and Connecticut marijuana dispensaries.

### **What Are the Reportable Controlled Substances?**

Drugs and other substances that are considered "controlled substances" under the federal Controlled Substances Act (CSA) are divided into five schedules (I-V). Substances are placed in their respective schedules based on: whether they have a currently accepted medical use in treatment in the United States, their relative abuse potential, and likelihood of causing dependence when abused. (See Appendix I)

Prescription information for the PMP database is collected for schedules II, III, IV and V controlled substances, as defined in state regulation.<sup>34</sup> An updated list of the schedules is published annually by the federal government and states are sent notices for upcoming changes. DCP reviews the anticipated changes and adopts regulations, accordingly.

State law exempts the reporting of samples of controlled substances dispensed by a physician to a patient or any controlled substances dispensed to inpatients in hospitals, nursing homes, or hospices.<sup>35</sup> An exemption also exists for any drug dispensed by a licensed health care facility provided the amount is for treatment of no more than 48 hours.

### **How Is Information Received, Stored, and Accessed Within PMP?**

Originally funded with two federal grants from the U.S. Department of Justice and the U.S. Department of Health and Human Services, the Connecticut Prescription Monitoring Reporting System (CPMRS) is a secure web-based system that allows prescribing practitioners, pharmacists, and law enforcement to view a patient's controlled substance history. The DCP commissioner contracts with Optimum Technology, Inc. (Optimum), an out-of-state vendor, to electronically collect controlled substance prescription information in accordance with state laws governing pharmacies. Figure 4 illustrates the flow of information in the database.

There are two aspects of the CPMRS: 1) data submission of reportable controlled substances to the system administrator, and 2) information access management handled by the program administrator. As seen in Figure 4, Optimum is the system administrator and DCP is the program administrator. This means that Optimum handles the information technology issues of uploading the electronic submissions from the mandated reporters and identifying any data

---

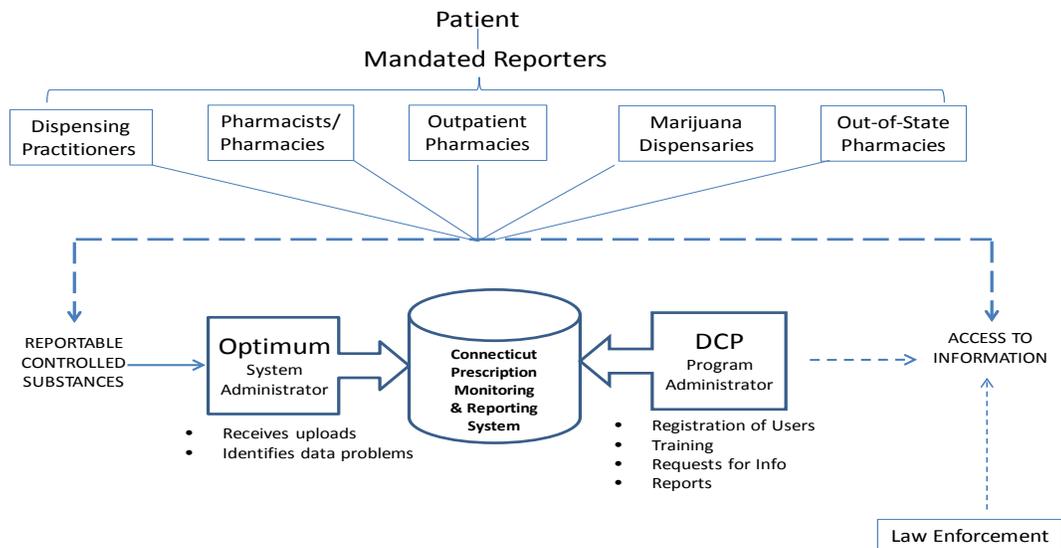
<sup>33</sup> Nonresident pharmacy is defined as any pharmacy located outside the state that ships, mails or delivers, in any manner, legend devices or legend drugs into this state pursuant to a prescription order (C.G.S. Sec. 20-627).

<sup>34</sup> Schedule I substances have: no currently accepted medical use in the United States, a lack of accepted safety for use under medical supervision, and a high potential for abuse.

<sup>35</sup> The exemption does not apply to assisted living facilities, home hospice, or hospice in an assisted living facility.

problems (e.g., conflicting, incomplete, or inaccurate data). DCP, as the program administrator, regulates the use and access of the database.

**Figure 4. Connecticut Prescription Monitoring & Reporting System Information Flow**



Source: PRI

**System administration.** The data submission process begins with a patient encounter with one or more mandated reporters. State law outlines what prescription information must be recorded and sent to CPMRS. The information is collected and submitted pursuant to the electronic reporting standard for prescription monitoring programs set out by the American Society for Automation in Pharmacy.

All mandated reporters must submit the information electronically according to a DCP-approved format. Current law allows for other DCP-approved methods of reporting by pharmacies, outpatient pharmacies, or dispensing prescribers that do not maintain electronic records. This includes computer disc or magnetic tape. According to DCP, almost all reporting is done by computer upload. Rarely, a mandated reporter may use an alternative submission method if there is a problem with the computer upload. All data submissions of any format are managed by Optimum. (The Optimum database server is located in Ohio and a backup server is located on-site but off-network at DCP.)

Currently, CPMRS receives data at least once per week from dispensing pharmacies and dispensing prescribers.<sup>36</sup> Starting July 1, 2016, state law requires them to report to the program immediately after dispensing controlled substances but in no event more than 24 hours after doing so.<sup>37</sup>

<sup>36</sup> Marijuana dispensaries are required to report daily.

<sup>37</sup> Pursuant to P.A. 15-5 (Sec. 354) June Special Session.

Once received, Optimum will identify any data problems and notify the mandated reporter to reconcile any data issues.

All prescription information submitted into CPMRS has been retained since its 2008 launch. Among the database security precautions in place include a 90-day password renewal which includes a strong password policy<sup>38</sup> and an audit feature requiring database registrants to revise/update their user information every three years. In addition, DCP may remove or restrict access of users who are no longer licensed or in good standing. Further evaluation of the DCP privacy safeguards will be included in the December report.

**Program administration.** In addition to community and professional outreach and educational activities, DCP manages the CPMRS program administration including processing of database registration applications, training, and setting up accounts, and handling access issues.

*Registration.* Registration is required of every authorized user of the database. Practitioners and pharmacists must obtain a DCP certificate of registration to access the electronic database. There is no cost for registering or accessing the system.

In 2013, state law was passed requiring all prescribers in possession of a Connecticut Controlled Substance Practitioner (CPS) registration to also register with PMP. According to DCP, approximately 15,760 (61 percent) of the 26,000 Connecticut prescribing practitioners have registered with PMP. The department has issued enforcement letters to the 39 percent non-compliant prescribers. Penalty for non-compliance can include the loss of the controlled substances registration. Penalties have not yet been issued.

*Training.* DCP provides a CPMRS data reporting manual to assist dispensing prescribers and pharmacies in properly uploading the required information. The manual contains all the information necessary to successfully upload the dispensing data into CPMRS. While Optimum handles issues with data submissions, PMP staff is available to assist with problems accessing registered accounts.

*Access to database.* All access to the CPMRS is controlled by DCP. As noted earlier, prescribing practitioners and pharmacists are allowed to access their own patients' prescription histories to help identify compliance and patterns of misuse, diversion, and/or abuse. Registration for access to the PMP database is also critical for compliance with state law.

Currently, Connecticut marijuana dispensaries must review a patient's PMP history before dispensing any medical marijuana. Beginning October 1, 2015, all prescribing practitioners must review a patient's PMP records prior to prescribing greater than a 72-hour supply of any controlled substance. Whenever controlled substances are prescribed for continuous or prolonged treatment, the prescriber must review the patient's PMP records at least once every 90 days.<sup>39</sup>

---

<sup>38</sup> A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly.

<sup>39</sup> P.A. 15-198.

Limited access is also statutorily allowed to law enforcement and regulatory personnel to assist with investigations related to doctor shopping, pharmacy shopping, and fraudulent activity. Only authorized members of law enforcement that are regularly involved in the narcotic/drug investigations are provided access after receiving database training. DCP may also consider requests for de-identified information from accredited researchers and other states under certain conditions. (Access management to the PMP database will be further explored in the December report.)

### **Facts and Statistics for Prescription Monitoring Program**

- All states, except Missouri, have a statewide prescription drug monitoring program.
- Federal grants are available to states for these programs through the U.S. Department of Justice and Department of Health and Human Services.
- Although these programs are federally supported, the Drug Enforcement Administration (DEA) is not involved with the administration of any state PMP.
- Approximately six million prescriptions are filled for controlled substances every year in Connecticut.
- As of September 17, 2015, there were a total of 40 million records contained in CPMRS.
- As of September 17, 2015, Connecticut registered CPMRS users included:
  - Prescribing practitioners (15,760)
  - Pharmacists (2,035)
  - Law Enforcement (343)
- There are 500 out-of-state pharmacies reporting to CPMRS.
- DCP has entered into memoranda of understanding (MOUs) with 17 other states to share prescription information. This information is limited to authorized prescribers and pharmacists.



# APPENDICES



---

## STUDY SCOPE

### Health Information Privacy in Selected State Programs

#### Focus

The study will focus on how health information privacy is maintained in selected state agency programs. Specifically, the study will evaluate the management of personal health information, including certain confidentiality requirements, at the Department of Public Health's (DPH) Infectious Diseases section and the Department of Consumer Protection's (DCP) Prescription Monitoring Program.

#### Background

In order to provide a wide range of public services, government agencies may be required to collect and maintain personal information on citizens and businesses. This may include privacy sensitive information such as home addresses, Social Security numbers, medical conditions, family relationships, biometric data (e.g., fingerprints, retina images), and personal finances.

Health information, in particular, has been subject to heightened concerns about confidentiality as many core public health activities rely on the acquisition, storage, and use of personal information. The Department of Consumer Protection oversees the prescription monitoring program, which collects prescription data from pharmacies and other dispensing practitioners for controlled substances into a central database called the Connecticut Prescription Monitoring and Reporting System (CPMRS). The purpose of the CPMRS is to help prevent and detect prescription drug misuse and diversion. The Department of Public Health's Infectious Diseases section collects data to assess chronic and infectious disease and associated risk factors, identifies and responds to emerging infections, and conducts outbreak investigations and surveillance. Given this study's completion date of early December 2015, the focus is only on these two programs.

State agencies must manage personal data in accordance with a variety of specific state and federal statutes that govern the public disclosure of this information. In addition, agencies are responsible for the personal data in their custody or under their control, even if the information is in the custody of private service providers or contractors.

Overall, state executive branch agencies are subject to the requirements of: 1) the state Personal Data Act, which primarily sets out a structure for state agency record maintenance and retention; and 2) the state Freedom of Information Act, which establishes a broad foundation to promote disclosure of agency records, with certain exemptions. In addition, many agencies must comply with laws focused on specific types of data. For example, the Health Insurance Portability and Accountability Act (HIPAA) provides federal protections for individually identifiable health information held by the government and other covered entities. It also gives patients an array of rights with respect to that information.

---

Public Act 15-142 requires the secretary of the Office of Policy and Management (OPM) to establish policies and procedures to protect and ensure the security, privacy, confidentiality, and administrative value of data collected and maintained by executive agencies. Further, the act establishes protocols to protect confidential information that a private contractor obtains from a state contracting agency.

There are many important management considerations regarding how state agency records are maintained. Included among these is the necessity to collect certain information, as well as how the information is used, accessed, shared, safeguarded, and stored. All state executive branch agencies are required under the Personal Data Act to have regulations that describe the agency's procedures regarding the maintenance and use of personal data.

### **Areas of Analysis**

- 1) Discuss the concept of information privacy and its relationship to confidentiality.
- 2) Describe the federal and state legal protections that relate to information privacy.
- 3) Identify and catalog what privacy sensitive health data is collected within the selected programs and examine:
  - a) why personal information is being collected and if the reason meets the requirements of Personal Data Act; and
  - b) how personal data is being collected, used, accessed, shared, safeguarded, and stored.
- 4) Review program regulations, policies, and procedures that protect and secure personal and confidential data to determine if:
  - a) the requirements of state and federal law are met;
  - b) mechanisms are in place to ensure compliance; and
  - c) clear lines of accountability exist for maintaining information privacy.
- 5) Evaluate information privacy requirements for private contractors that may receive confidential health information and how those requirements are monitored.
- 6) Review interagency and intergovernmental agreements for handling privacy issues and determine if they are consistent with applicable federal and state privacy laws.

### **Areas Not Under Review**

The study will not include an overall performance evaluation of the selected state agency programs.

#### **PRI Staff Contacts**

Scott Simoneau: [Scott.Simoneau@cga.ct.gov](mailto:Scott.Simoneau@cga.ct.gov)  
Michelle Castillo: [Michelle.Castillo@cga.ct.gov](mailto:Michelle.Castillo@cga.ct.gov)  
Alexis Warth: [Alexis.Warth@cga.ct.gov](mailto:Alexis.Warth@cga.ct.gov)

## Appendix B: Department and Program Specific Laws and Regulations

	Citation	Summary
<b>DPH</b>	C.G.S. Sec. 19a-215	Establishes reportable disease program; includes language providing confidentiality of data (§19a-215(5)(e))
	C.G.S. Sec. 19a-262	Mandates reporting of tuberculosis cases, including what information is required in report
	C.G.S. Sec. 19a-7(h)	Establishes the Childhood Immunization Registry
	C.G.S. Sec. 19a-25	Governs confidentiality of IDS records: “All information, records of interviews, written reports, statements, notes, memoranda or other data...procured by the Department of Health...in connection with studies of morbidity and mortality conducted by the Department of Public Health...or procured by the directors of health of towns, cities or boroughs or the Department of Public Health pursuant to section 19a-215...for the purpose of reducing the morbidity or mortality from any cause or condition, shall be confidential.”
	Conn. Agency Regs. Secs. 19a-2a-1 to 19a-2a-23	Describes personal data systems within DPH. Refer to §19a-2a-12 for specific information about infectious disease epidemiology data system
	Conn. Agency Regs. Secs. 19a-25-1 to 19a-25-4	Regulates disclosure of health data and the use of health data for enforcement purposes
	Conn. Agency Regs. Secs. 19a-36-A1 to A56	Regulates use of Reportable Diseases and Laboratory Findings
<b>DCP</b>	C.G.S. Sec. 21a-254	Establishes PMP, including who is a mandated reporter, what information is required, and the establishment of the electronic monitoring system
	C.G.S. Sec. 21a-317	Describes requirement for any practitioner who distributes, administers, or dispenses any controlled substances to register for PMP
	C.G.S. Sec. 20-578	Confidentiality clause for PMP records: “Information received by the department...through filed reports or inspection or as otherwise authorized...shall not be disclosed publicly in such a manner as to identify individuals or institutions.”
	Conn. Agency Reg. Sec. 21a-1-7a	Description of the personal data systems used at DCP. PMP is not listed in this section
	Conn. Agency Regs. Secs. 21a-254-1 to 21a-254-7	Outlines general requirements, evaluation, and management of the electronic monitoring program
	Conn. Agency Regs. Secs. 21a-326-1 to 21a-326-5	Outlines details of registration process and responsibilities of registrants
	Source: PRI	



# Appendix C

---

## Health Insurance Portability and Accountability Act (HIPAA)

Neither IDS or PMP are covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). However, an understanding of HIPAA is helpful in a broader discussion of information privacy and security. HIPAA was adopted to ensure health insurance coverage after leaving an employer and to provide standards for facilitating healthcare related electronic transactions. Prior to the passage of HIPAA, patient privacy was primarily addressed in a piecemeal fashion through various federal and state laws. HIPAA established a set of privacy and security standards that created a “national minimum of basic protections” for individuals, while still allowing for necessary data collection and sharing for public health and safety purposes.<sup>40</sup> There are two sections in HIPAA that specifically apply to personal health information privacy and security, commonly referred to as the Privacy Rule (45 C.F.R. §§164.500-534) and Security Rule (45 C.F.R. §§164.302-318).

### Covered Entities

The Privacy Rule and the Security Rule apply only to specific entities, referred to as “covered entities” that fall into three categories:

- Health Plans – Individual or group health plans provided by either private entities or government organizations (e.g., Medicaid, Medicare, or Veterans Health)
- Healthcare Clearinghouses – A public or private entity, including a billing service, repricing company or community health information system, that processes nonstandard data or transactions into standard transactions or data elements.
- Healthcare Providers – A provider of healthcare services and any other person or organization that furnishes, bills or is paid for healthcare in the normal course of business. Providers (physicians, hospital, clinics, etc.) are only considered covered entities if they transmit health information in an electronic form.<sup>41,42</sup>

---

<sup>40</sup> Centers for Disease Control and Prevention. *HIPAA Privacy Rule and public health: Guidance from CDC and the U.S. Department of Health and Human Services*. MMWR 2003;52 (Early Release), <http://www.cdc.gov/privacyrule/Guidance/PRmmwrguidance.pdf>

<sup>41</sup> 45 C.F.R. §160.103.

<sup>42</sup> Requirements are also extended to “nonemployee business associates” of covered entities, including lawyers, accountants, billing companies and other contractors who require the exchange of private health information to provide the contracted service (45 C.F.R. §164.500c).

---

The regulations under the Privacy Rule do not cover employers, certain insurers (auto, life and worker compensation), or public agencies that deliver social security or welfare benefits.<sup>43</sup>

## **Protected Health Information (PHI)**

Protected health information (PHI) is defined as any individually identifiable health information that is transmitted or maintained in any form (electronic, paper or oral).<sup>44</sup> In order for information to be considered PHI, it must relate to: past, present, or future physical or mental health; the provision of healthcare to an individual; or payment for the provision of healthcare to an individual. PHI can be identifiable in a number of ways, either as a single piece of identifying information (such as a Social Security number or fingerprint) or a combination of information that together could lead to the identification of an individual (e.g., name, date of birth, or zip code).

HIPAA lists 18 identifiers that must be removed in order for a dataset to be considered “de-identified;” including name, date of birth, telephone numbers, Social Security numbers, medical record numbers, vehicle identifiers, IP addresses, and biometric identifiers (such as fingerprints). While some types of information can clearly be labeled as personally identifying, it is the responsibility of covered entities to protect any information that could “reasonably” be used to identify an individual. It is important for any entity utilizing health information to consider how a combination of information could lead to the identification of an individual, especially in scenarios with small sample or population sizes.<sup>45</sup>

## **Privacy Rule**

The HIPAA Privacy Rule (Standards for Privacy of Individually Identifiable Health Information) provides covered entities with standards for the handling of protected health information. The Privacy Rule includes requirements that are intended to:

- give patients more control over their health information;
- set boundaries on the use and release of health records;
- establish appropriate safeguards that the majority of healthcare providers and others must achieve to protect the privacy of health information;
- strike a balance when public health responsibilities support disclosure of certain forms of data; and
- generally limit releases of information to the minimum reasonably needed for the purpose of the disclosure.<sup>46</sup>

---

<sup>43</sup> Centers for Disease Control and Prevention. *HIPAA Privacy Rule and public health: Guidance from CDC and the U.S. Department of Health and Human Services*. MMWR 2003;52 (Early Release), <http://www.cdc.gov/privacyrule/Guidance/PRmmwrguidance.pdf>

<sup>44</sup> 45 C.F.R. §160.103

<sup>45</sup> 45 C.F.R. §164.514(b)(1)(i)

<sup>46</sup> Centers for Disease Control and Prevention. *HIPAA Privacy Rule and public health: Guidance from CDC and the U.S. Department of Health and Human Services*. MMWR 2003;52 (Early Release)

---

In order to achieve these goals, HIPAA outlines requirements that must be followed by covered entities, including:

- notifying individuals regarding their privacy rights and how their information will be used and/or disclosed;
- adopting and implementing internal privacy policies and procedures;
- training employees to understand these policies and use them appropriately;
- designating individuals who are responsible for implementation of privacy policies and will respond to privacy related complaints or concerns;
- establishing privacy requirements to be included in contracts with third-parties who will receive PHI or who participate in covered activities; and
- establishing and implementing acceptable administrative, technical, and physical safeguards to protect PHI.

Under the Privacy Rule, covered entities are not permitted to release a patients' PHI without prior authorization from the patient, unless the disclosure falls into one of the following scenarios:

- release is required by federal, tribal, state, or local law(s);
- public health purposes (discussed below);
- health research, under certain circumstances and only if certain requirements are satisfied;
- abuse, neglect, or domestic violence – many states have mandated reporter laws that require providers to report safety concerns to the appropriate authorities;
- law enforcement, under certain circumstances, including a court order, subpoena or other legal order;
- judicial and administrative proceedings;
- organ, eye, or tissue donation purposes, only if the donor is deceased;
- health oversight purposes; and
- worker's compensation.<sup>46</sup>

### **Public Health Purpose Disclosures<sup>47</sup>**

One of the most widely used exemptions to the prior authorization requirements in HIPAA is for activities to ensure public health and safety.<sup>48</sup> Public health authorities,<sup>49</sup> including local, state, and federal organizations/offices, are authorized to receive and utilize PHI to identify, monitor, and respond to disease, death, and disability among populations. Therefore,

---

<sup>47</sup> Additional acceptable disclosure purposes can be found in 45 C.F.R. §160.203 and 45 C.F.R. §164.512.

<sup>48</sup> 45 C.F.R. §164.512.

<sup>49</sup> Public health authority is defined in HIPAA as “an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, that is responsible for public health matters as part of its official mandate” (45 C.F.R. §164.501).

---

covered entities may share PHI with authorized public health entities without authorization or permission from the individual patient. The covered entity is also exempt from the *minimum necessary information* standard of HIPAA when reporting to public health authorities.<sup>50</sup>

Whether or not a public health organization is considered a covered entity under HIPAA depends on the activities conducted by the organization. If a public health organization conducts any activities that are considered “covered” by HIPAA, such as directly providing health coverage or health services to individuals, the entity (or parts of) can be considered “covered.” Thus, a public health authority that has sections or programs that conduct covered activities can be considered a “covered entity” in part or in whole.

While the provision of PHI to a public health authority must meet the standards and requirements outlined in the Privacy Rule, once the information is provided to the health authority it is to be maintained, used, and disclosed consistent with the laws, regulations and policies applicable to the public health authority by state or local law.<sup>51</sup>

## Security Rule

The *Security Standards for Protection of Electronic Protected Health Information* section of HIPAA’s regulation provides standards, specifications, and requirements for the handling of electronic PHI by covered entities. The general requirements within the Security Rule are that the covered entity:

- ensures the confidentiality, integrity, and availability of all electronic PHI that the covered entity creates, receives, maintains, or transmits;
- protects against any reasonably anticipated threats or hazards to the security or integrity of such information;
- protects against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and
- ensures compliance with these standards by its workforce.<sup>52</sup>

The Security Rule includes specifications for administrative, physical, and technical safeguards, as well as organizational, policy, and procedural requirements. The safeguards are categorized as either *required*, meaning all covered entities are mandated to comply, or *addressable*, meaning an entity should evaluate if the safeguard is reasonable and appropriate for its environment.<sup>53</sup> If an entity establishes that it will not be adhering to standards that are labeled as *addressable*, it must document the assessment and reason for the lack of compliance.<sup>54</sup> The Security Rule mandates that covered entities establish, document, and distribute policies and procedures that ensure compliance with safeguards and standards.<sup>55</sup>

---

<sup>50</sup> 45 C.F.R.164.502(b)(2)(iii).

<sup>51</sup> Applicable only to authorities or programs within authorities who are considered “non-covered” entities. Topic discussed in *CDC MMWR*, Volume 52, April 11, 2003. Based off of 45 C.F.R. §160.203 and 45 C.F.R. §164.512(b)

<sup>52</sup> 45 C.F.R. §164.306.

<sup>53</sup> 45 C.F.R. §164.306(d).

<sup>54</sup> 45 C.F.R. §164.306(d).

<sup>55</sup> 45 C.F.R. §164.316.

---

## Protected Health Information Variables from HIPAA – 45 C.F.R. §164.514(b)(2)(i)

- Names
- All geographic subdivisions smaller than a state, including county, city, street address, precinct, zip code and equivalent geocodes
- All elements of date (except year) directly related to an individual; all ages >89 and all elements of dates (including year) indicative of such age (except for an aggregate into a single category of age >90)
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health-plan beneficiary numbers
- Account numbers
- Certificate and license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Medical device identifiers and serial numbers
- Internet universal resource locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers including fingerprints and voice prints
- Full-face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code, except that covered identities may, under certain circumstances, assign a code or other means of record identification that allows de-identified information to be re-identified

There is an exception in HIPAA allowing certain PHI to be included, without prior authorization, in a limited data set for public health, research or healthcare operations. This exception applies to information concerning a town or city, state and zip code, as well as elements of dates related to a person (e.g., years, birth dates, admission dates, discharge dates, and dates of death).<sup>56</sup>

---

<sup>56</sup> Centers for Disease Control and Prevention. *HIPAA Privacy Rule and public health: Guidance from CDC and the U.S. Department of Health and Human Services*. MMWR 2003;52 (Early Release)



# Appendix D

---

## Freedom of Information Act (FOIA)

The Connecticut Freedom of Information Act (FOIA) “provides the public with rights of access to records and meetings of public agencies,” as long as access is not restricted by federal or state law.<sup>57</sup> The overall goal of FOIA is to increase the transparency and accountability of government entities by allowing the public access to information. Members of the public are able to request copies or the opportunity to review records maintained by public agencies, as well as the opportunity to attend meetings held by public agencies. If an individual believes their FOIA rights have been violated, they have the right to appeal an agency’s denial of access to the FOI Commission (FOIC). The FOIC is made up of nine members and is charged with ensuring citizen access to public records and meetings.

Requests for information are made directly to the agency of interest, which are required to respond in a “prompt” manner. According to the FOIC, “prompt” is defined depending on “how busy the agency is at the time of the request, how time-consuming it will be to comply with the request and the urgency of need for the information contained in the records.” If a FOIA request is denied, the agency denying the request must notify the requestor, in writing, within four or ten business days of the request, depending on the reason for denial.<sup>58</sup>

### Exemptions

State law (C.G.S. Sec.1-210) outlines what public records are considered exempt from FOIA requests. The three exemptions that are relevant to this report are:

- personnel or medical files and similar files the disclosure of which would constitute an invasion of personal privacy ( C.G.S. Sec. 1-210(b)(2));
- records concerning an ongoing investigation by a municipal health authority or district department of health, prior to the completion of the investigation or within 30 days of the FOIA request, whichever comes first (C.G.S. Sec. 1-210(b)(16)); and
- records of standards, procedures, processes, software and codes, not otherwise available to the public, the disclosure of which would compromise the security or integrity of an information technology system (C.G.S. Sec. 1-210(b)(20)).

### Department Applicability

In addition to the exemptions listed in FOIA, there is language within C.G.S. Sec. 19a-25 that describes the confidentiality of information collected in investigations by the Department of Public Health. Specifically, C.G.S. Sec. 19a-25 states that:

---

<sup>57</sup> Connecticut FOIA Commission Citizen’s Guide, 2008.

<sup>58</sup> C.G.S. Sec. 1-206.

---

All information, records of interviews, written reports, statements, notes, memoranda or other data ...procured by the Department of Public Health ... in connection with studies of morbidity and mortality conducted by the Department of Public Health ... or procured by the directors of health of towns, cities or boroughs or the Department of Public Health pursuant to section 19a-215, ... for the purpose of reducing the morbidity or mortality from any cause or condition, shall be confidential.

The universality of the confidentiality authorized by C.G.S. Sec. 19a-25 was addressed in a 1999 Supreme Court case, *Babcock v. Bridgeport Hospital* (251 Conn.790). That decision stated that “the privilege afforded by 19a-25 is limited to the designated materials of a hospital staff committee that are generated primarily for the purpose of the study of morbidity and mortality, undertaken specifically for the purpose of reducing the incidence of patient deaths.”<sup>59</sup> The *Babcock* decision distinguishes that the confidentiality afforded by C.G.S. Sec. 19a-25 is only relevant to information collected *primarily* for the purpose of the study of morbidity and mortality and with the *specific purpose* of reducing patient death, removing the blanket confidentiality afforded prior to this decision.

While this ruling was an interpretation of how the statute applies specifically to hospital committees, the impact can be seen within multiple FOIC decisions granting requestors access to information that was ruled as not being *primarily* collected for the purpose of reducing patient death.<sup>60</sup> In a May 2015 FOIC decision, the commission ruled that information reported to the Department of Public Health by a local health department concerning a foodborne illness outbreak was considered confidential under C.G.S. Sec. 19a-25, because although enforcement might have been one reason for the activity, the particular and primary purpose was to reduce morbidity and mortality from the suspected outbreak.<sup>61</sup> The FOIC has generally continued to deny requests for information collected through the reporting or investigation of reportable diseases, citing C.G.S. Sec. 19a-25 and Sec. 19a-125.<sup>62</sup>

Records collected or maintained by PMP are considered exempt from FOIA requirements due to the language found in C.G.S. Sec. 1-210(b)(2) (medical or personnel files), as well as C.G.S. Sec. 20-578, which states that “information received by the department, through filed reports or inspection or as otherwise authorized under chapters 418 and 420b, shall not be disclosed publicly in such a manner as to identify individuals or institutions.” Chapter 420b contains state law that created PMP, therefore limiting the public release of records from that program.

---

<sup>59</sup> *Babcock v. Bridgeport Hospital*, 251 Conn. 790 (1999).

<sup>60</sup> A 1997 FOIC decision (FIC 1997-092) denied a requestor de-identified and aggregated abortion information from a Connecticut hospital on the basis of C.G.S. Sec.19a-25. A similar request for de-identified and aggregated abortion information was granted in 2004 (FIC 2004-552) based on the language of the *Babcock* decision.

<sup>61</sup>FIC 2014-435.

<sup>62</sup>See, e.g., FIC 2000-581, FIC 2002-307, FIC 2009-307, FIC 2014-435, FIC 2014-519 and FIC 2014-783.

# Appendix E

---

## Personal Data Act (PDA)

The Personal Data Act was passed in Connecticut in 1976 with the intent of establishing responsibilities and standards for data collection, usage and storage within state and municipal agencies. In this act, *personal data* is defined as “any information about a person’s education, finances, medical or emotional condition or history, employment or business history, family or personal relationships, reputation of character which because of name, identifying number, mark or description can be readily associated with a particular person.”<sup>63</sup> Due to the broad definition of personal data, this act impacts many more agencies than a sector specific law, such as HIPAA. The standards and regulations outlined in the Personal Data Act apply to all state or municipal boards, commissions, departments or officers, with the exception of the legislature, courts, governor, lieutenant governor, attorney general and town or regional boards of education.<sup>64</sup>

The primary responsibilities and standards in the Personal Data Act include that state and municipal agencies must:

- inform each employee who has access to personal data of the provisions in the Personal Data Act, the agency’s regulations, FOIA and any other federal or state statutes regarding personal information;
- take reasonable precautions to protect personal data from fire, theft, flood, natural disaster, or other physical threats;
- keep a record of any individual, agency, or organization who obtains access to personal data and the reason for this access;
- maintain the minimum amount of information necessary to complete the purpose of the agency;
- disclose to a person, upon written request, all personal data concerning him/her that is maintained by the agency, as well as any record of authorized disclosures of information; and
- establish regulations that describe the general nature and purpose of each personal data system, categories of information that are collected/kept, and procedures concerning the maintenance of data.<sup>65</sup>

## Access to Individual/Own Information

Generally an individual has a right to see all personal data concerning himself/herself, but an agency does have the right to refuse. An agency can refuse a FOIA request if it is believed that the disclosure of information would be detrimental to that person or if the refusal is

---

<sup>63</sup> C.G.S. Sec. 4-190(9)

<sup>64</sup> C.G.S. Sec. 4-190(1)

<sup>65</sup> C.G.S. Sec. 4-193

---

permitted or required by other federal or state law.<sup>66</sup> There are two primary mechanisms an individual has to contest a refusal to release information: (1) request that a qualified medical doctor review the information to determine if a release will be detrimental to the physical, mental, or emotional health of the individual or (2) petition the Superior Court for the judicial district in which the individual resides.<sup>67</sup>

Under the Personal Data Act, an individual has the right to contest the accuracy, completeness, or relevancy of his/her personal data.<sup>68</sup> If the agency disputes any changes requested by an individual, the person has the right to submit a letter outlining his/her concerns and corrections, which then becomes a permanent part of the agency's personal data system.

## **Recent Changes**

In 2015, the Connecticut legislature passed An Act Improving Data Security and Agency Effectiveness.<sup>69</sup> This act created and amended the following requirements for agencies and businesses operating in Connecticut:

- requires notice to affected individuals and the Connecticut attorney general within 90 days of a security breach;
- adds biometric data, such as fingerprints, retina scans, and voice prints, to the definition of personal information;
- requires all businesses, including health insurers, to offer one year of identity theft protection services to affected individuals following any data breach; and
- requires health insurers and any contractor who receives personal information from state agencies to implement and maintain minimum data security safeguards.

The act also includes specific security requirements for health insurers and state contractors. These security requirements do not apply to DPH or DCP.

---

<sup>66</sup> C.G.S. Sec. 4-194

<sup>67</sup> C.G.S. Secs. 4-194(b) to 4-195

<sup>68</sup> C.G.S. Sec. 4-193(h)

<sup>69</sup> Public Act No. 15-142

---

# Appendix F

REPORTABLE DISEASES, EMERGENCY ILLNESSES and HEALTH CONDITIONS - 2015		
<p>The Commissioner of the Department of Public Health (DPH) is required to declare an annual list of Reportable Diseases, Emergency Illnesses and Health Conditions. The Reportable Disease Confidential Case Report form (PD-23) or other disease specific form should be used to report the disease, illness, or condition. Reports (mailed, faxed, or telephoned into the DPH) should include the full name and address of the person reporting and attending physician, name of disease, illness or condition, and full name, address, date of birth, race/ethnicity, gender and occupation of the person affected. Forms can be found on the DPH <a href="#">website</a>. See page 4 for a list of persons required to report Reportable Diseases, Emergency Illnesses and Health Conditions. Mailed reports must be sent in envelopes marked "CONFIDENTIAL." Changes for 2015 are noted in <b>bold</b> and with an asterisk (*).</p>		
<p><b>Category 1 Diseases:</b> Report immediately by telephone on the day of recognition or strong suspicion of disease for those diseases marked with a telephone (☎). Also mail a report within 12 hours.</p> <p><b>Category 2 Diseases:</b> Diseases not marked with a telephone are Category 2 diseases. Report by mail within 12 hours of recognition or strong suspicion of disease.</p>		
<ul style="list-style-type: none"> <li>☎ Acquired Immunodeficiency Syndrome (1,2)</li> <li>☎ Anthrax</li> <li>☎ Babesiosis</li> <li>☎ Botulism</li> <li>☎ Brucellosis</li> <li>California group arbovirus infection</li> <li>Campylobacteriosis</li> <li>Carbon monoxide poisoning (3)</li> <li>Chancroid</li> <li>Chickenpox</li> <li>Chickenpox-related death</li> <li><b>Chikungunya *</b></li> <li>Chlamydia (<i>C. trachomatis</i>) (all sites)</li> <li>☎ Cholera</li> <li>Cryptosporidiosis</li> <li>Cyclosporiasis</li> <li>Dengue</li> <li>☎ Diphtheria</li> <li>Eastern equine encephalitis virus infection</li> <li><i>Ehrlichia chaffeensis</i> infection</li> <li><i>Escherichia coli</i> O157:H7 gastroenteritis</li> <li>Gonorrhea</li> <li>Group A Streptococcal disease, invasive (4)</li> <li>Group B Streptococcal disease, invasive (4)</li> <li><i>Haemophilus influenzae</i> disease, invasive all serotypes (4)</li> <li>Hansen's disease (Leprosy)</li> <li>Healthcare-associated Infections (5)</li> <li>Hemolytic-uremic syndrome (6)</li> <li>Hepatitis A</li> <li>Hepatitis B               <ul style="list-style-type: none"> <li>• acute infection (2)</li> <li>• HBsAg positive pregnant women</li> </ul> </li> <li>Hepatitis C               <ul style="list-style-type: none"> <li>• acute infection (2)</li> <li>• positive rapid antibody test result</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>HIV-1 / HIV-2 infection in (1)               <ul style="list-style-type: none"> <li>• persons with active tuberculosis disease</li> <li>• persons with a latent tuberculous infection (history or tuberculin skin test <math>\geq 5</math>mm induration by Mantoux technique)</li> <li>• persons of any age</li> <li>• pregnant women</li> </ul> </li> <li>HPV: biopsy proven CIN 2, CIN 3 or AIS or their equivalent (1)</li> <li>Influenza-associated death</li> <li>Influenza-associated hospitalization (7)</li> <li>Lead toxicity (blood level <math>\geq 15</math> <math>\mu</math>g/dL)</li> <li>Legionellosis</li> <li>Listeriosis</li> <li>Lyme disease</li> <li>Malaria</li> <li>☎ Measles</li> <li>☎ Melioidosis</li> <li>☎ Meningococcal disease</li> <li>Mercury poisoning</li> <li>Mumps</li> <li>Neonatal bacterial sepsis (8)</li> <li>Neonatal herpes (<math>\leq 60</math> days of age)</li> <li>Occupational asthma</li> <li>☎ Outbreaks:               <ul style="list-style-type: none"> <li>• Foodborne (involving <math>\geq 2</math> persons)</li> <li>• Institutional</li> <li>• Unusual disease or illness (9)</li> </ul> </li> <li>☎ Pertussis</li> <li>☎ Plague</li> <li>Pneumococcal disease, invasive (4)</li> <li>☎ Poliomyelitis</li> <li>☎ Q fever</li> <li>☎ Rabies</li> <li>☎ Ricin poisoning</li> <li>Rocky Mountain spotted fever</li> </ul>	<ul style="list-style-type: none"> <li>Rotavirus</li> <li>☎ Rubella (including congenital)</li> <li>Salmonellosis</li> <li>☎ SARS-CoV</li> <li>Shiga toxin-related disease (gastroenteritis)</li> <li>Shigellosis</li> <li>Silicosis</li> <li>☎ Smallpox</li> <li>St. Louis encephalitis virus infection</li> <li>☎ Staphylococcal enterotoxin B pulmonary poisoning</li> <li>☎ <i>Staphylococcus aureus</i> disease, reduced or resistant susceptibility to vancomycin (1)</li> <li><i>Staphylococcus aureus</i> methicillin-resistant disease, invasive, community acquired (4,10)</li> <li><i>Staphylococcus epidermidis</i> disease, reduced or resistant susceptibility to vancomycin (1)</li> <li>Syphilis</li> <li>Tetanus</li> <li>Trichinosis</li> <li>☎ Tuberculosis</li> <li>☎ Tularemia</li> <li>Typhoid fever</li> <li>Vaccinia disease</li> <li>☎ Venezuelan equine encephalitis</li> <li><i>Vibrio</i> infection (<i>parahaemolyticus</i>, <i>vulnificus</i>, other)</li> <li>☎ Viral hemorrhagic fever</li> <li>West Nile virus infection</li> <li>☎ Yellow fever</li> </ul>
<p><b>FOOTNOTES:</b></p> <ol style="list-style-type: none"> <li>1. Report only to State.</li> <li>2. CDC case definition.</li> <li>3. Includes persons being treated in hyperbaric chambers for suspect CO poisoning.</li> <li>4. Invasive disease: confirmed by isolation from sterile fluid (blood, CSF, pericardial, pleural, peritoneal, joint, or vitreous) bone, internal body sites, or other normally sterile site including muscle.</li> <li>5. Report HAIs according to current CMS pay-for-reporting or pay-for-performance requirements. Detailed instructions on the types of HAIs, facility types and locations, and methods of reporting are available on the DPH website: <a href="http://www.ct.gov/dph/HAI">www.ct.gov/dph/HAI</a>.</li> <li>6. On request from the DPH and if adequate serum is available, send serum from patients with HUS to the DPH Laboratory for antibody testing.</li> <li>7. Reporting requirements are satisfied by submitting the Hospitalized and Fatal Cases of Influenza—Case Report Form to the DPH in a manner specified by the DPH.</li> <li>8. Clinical sepsis and blood or CSF isolate obtained from an infant <math>\leq 72</math> hours of age.</li> <li>9. Individual cases of "significant unusual illness" are also reportable.</li> <li>10. Community-acquired: infection present on admission to hospital, and person has no previous hospitalizations or regular contact with the health-care setting.</li> </ol>		
<p><b>How to report:</b> The PD-23 is the general disease reporting form and should be used if other specialized forms are not available. The PD-23 can be found for download from the DPH website (<a href="http://www.ct.gov/dph/forms">www.ct.gov/dph/forms</a>). It can also be ordered in triplicate by writing the Department of Public Health, 410 Capitol Ave., MS#11EPI, P.O. Box 340308, Hartford, CT 06134-0308 or by calling the Epidemiology and Emerging Infections Program (860-509-7994). Specialized reporting forms from the following programs are available on the DPH website or by calling the following telephone numbers: <a href="#">HIV/AIDS Surveillance</a> (860-509-7900), <a href="#">Sexually Transmitted Disease Program</a> (860-509-7920), <a href="#">Tuberculosis Control Program</a> (860-509-7722), <a href="#">Occupational Health Surveillance Program</a> (860-509-7740), <a href="#">Hospitalized and Fatal Cases of Influenza</a> through the Epidemiology and Emerging Infections Program (860-509-7994).</p> <p><b>Telephone reports</b> of Category 1 disease should be made to the local director of health for the town in which the patient resides and to the Epidemiology and Emerging Infections Program (860-509-7994). Tuberculosis cases should be directly reported to the Tuberculosis Control Program (860-509-7722). For the name, address, or telephone number of the local Director of Health for a specific town contact the Office of Local Health Administration (860-509-7660). For public health emergencies, an epidemiologist can be reached evenings, weekends, and holidays through the DPH emergency number (860-509-8000).</p>		



## Appendix G

### Infectious Disease Databases (As of September 25, 2015)

Unit/ Program	Project	Purpose: Surveillance/ Research	Activity/Disease tracked/Study name	Database Name	IT Platform	Responsible Party (Creator)	Location of Database	Remote Access to Database (Y/N)
Epidemiology (EPI)/Emerging Infections Program (EIP)	Active Bacterial Core	Surveillance	H. influenza, N. meningitidis, Group A Streptococcus (GAS), Group B Streptococcus (GBS) and Streptococcus pneumonia	CTEDSS ABCs surveillance	Proprietary and CDC developed EpiInfo/Access database	DPH/CDC	DPH/BEST	CTEDSS = YES ABCs surveillance = NO
EPI/EIP	Active Bacterial Core	Surveillance	Legionella	CTEDSS ABCs surveillance	Proprietary and CDC developed EpiInfo/ Access	DPH/CDC	DPH/BEST	CTEDSS = YES ABCs surveillance = NO
EPI/EIP	Active Bacterial Core	Surveillance	Neonatal sepsis	ABCs surveillance	CDC developed EpiInfo/Access	CDC	DPH	NO
EPI/EIP	Active Bacterial Core	Research	Pneumococcal Conjugate Vaccine (PCV13) (Research study)	ABCs PCV13	CDC developed Access	CDC	DPH	NO
EPI/EIP	Active Bacterial Core	Surveillance	Methicillin-resistant Staphylococcus aureus (MRSA)	MRSA study	CDC developed Access	CDC	DPH	NO
EPI/EIP	Active Bacterial Core	Surveillance	Pneumococcal (urine antigen)	Pneumococcal urine antigen study	Research Electronic Data Capture (REDCAP) a Vanderbilt University software product	CDC	CDC	YES with Secure Access Management System (SAMS) credentials issued by CDC
EPI/EIP	Pertussis	Surveillance	Enhanced Bordetella pertussis surveillance	CTEDSS Pertussis study	Proprietary and CDC developed Access database	CDC	DPH	CTEDSS = YES ABCs surveillance = NO

Unit/ Program	Project	Purpose: Surveillance/ Research	Activity/Disease tracked/Study name	Database Name	IT Platform	Responsible Party (Creator)	Location of Database	Remote Access to Database (Y/N)
EPI/EIP	Flu	Surveillance	Flu SurvNet	Influenza Hospitalization Surveillance Network 2014-15	Access	CDC	Yale EIP	NO
EPI/EIP	Flu	Surveillance	Pediatric Antiviral Impact	1) FluSurv-NET anti-viral (AV) study database 2010-11 and 2011-12 2) FluSurv-NET AV study database 2012-13	Access	CDC	Yale EIP	NO
EPI/EIP	Flu	Surveillance	Flu Surveillance Case finding	CTEDSS	Proprietary	DPH	DPH/BEST	YES
EPI/EIP	FoodNet	Surveillance	Campylobacter, Listeria, Salmonella, Shiga toxin-producing E. coli (STEC) O157 and non-O157 STEC, Shigella, Vibrio, Yersinia, Cyclospora, Cryptosporidium,	CTEDSS	Proprietary	DPH	DPH/BEST	YES
EPI/EIP	FoodNet	Research	Lab Survey (of clinical laboratories in CT that test for foodborne pathogens)	FoodNet Lab Survey	Research Electronic Data Capture (REDCAP) a Vanderbilt University software product	CDC	CDC	YES with Secure Access Management System (SAMS) credentials issued by CDC
EPI/EIP	FoodNet	Surveillance	Population-based Hemolytic Uremic Syndrome (HUS)	HUS Surveillance	Access	CDC	Yale EIP	NO
EPI/EIP	FoodNet	Research	Shiga toxin-producing E. coli (STEC) non-O157 Research Study	STEC Case-Control Study	Access	CDC	Yale EIP	NO

Unit/ Program	Project	Purpose: Surveillance/ Research	Activity/Disease tracked/Study name	Database Name	IT Platform	Responsible Party (Creator)	Location of Database	Remote Access to Database (Y/N)
EPI/EIP	Clostridium difficile (C. diff)	Surveillance	Core Surveillance	Incident Case Detection System (ICDS)/Incident Case Management System (ICMS)	.NET Web Application	CDC	Yale EIP/CDC	YES with Secure Access Management System (SAMS) credentials issued by CDC
EPI/EIP	C. diff	Research	Research Study (LTC survey)	Long Term Care Facility (LTC) survey	Access	Yale	Yale EIP	NO
EPI/EIP	Healthcare Associated Infections-Community Interface (HAIC)	Surveillance	Point prevalence (IV)	Healthcare facility assessment form	Research Electronic Data Capture (REDCAP) a Vanderbilt University software product	CDC	CDC	YES (with Secure Access Management System (SAMS) credentials issued by CDC)
EPI/EIP	human papillomavirus (HPV)	Surveillance	HPV vaccine impact surveillance database	HPV	Access	CDC	Yale EIP	NO
EPI/EIP	HPV	Research	HPV enhanced data collection	HPV	Access	CDC	Yale EIP	NO
EPI/EIP	HPV	Research	HPV interviews	HPV	Access	CDC	Yale EIP	NO
EPI/EIP	TickNet	Research	Acaracide Study	LTDPS & LTDPS 2012	Access	CDC	Yale EIP	NO
EPI/EIP	TickNet	Research	Bait Box Intervention Study	LTDPS Bait Box Intervention	Access	CDC	Yale EIP	NO
EPI/EIP	TickNet	Research	Cost of Lyme Disease Study	COLD Study	Access	CDC	Yale EIP	NO
Healthcare Associated Infections (HAI)	HAI	Surveillance	CLABSI, CAUTI, MRSA, CDI	NHSN	NHSN	CDC	CDC	YES (with Secure Access Management System (SAMS) credentials issued by CDC)

Unit/ Program	Project	Purpose: Surveillance/ Research	Activity/Disease tracked/Study name	Database Name	IT Platform	Responsible Party (Creator)	Location of Database	Remote Access to Database (Y/N)
HAI	HAI	Surveillance	Drug resistant bacteria	CRE database	Access	DPH	DPH	No
HCSS	Ryan White	Surveillance	Individuals receiving services under federal grant program	Care Ware	Windows/SQL	HRSA/HAB	City of Hartford	Yes
HIV Surveillance	human immunodeficiency virus (HIV)	Surveillance	Diagnosed HIV or AIDS	eHars	SQL	CDC	DPH	Yes
HIV Surveillance	HIV	Surveillance	HIV	HARMS	SQL	DPH	DPH	No
HIV Prevention	HIV	Surveillance/ Prevention Case management/ Monitoring and Evaluation	Aids prevention activities including HIV testing	Evaluation Web		CDC/Luther Consulting LLC	Indianapolis	Yes
HIV Prevention	HIV	Monitoring and Evaluation	Harm Reduction Activities/ Syringes Exchange Service/ HIV Prevention/Naloxone Distribution/	XeringaX DB v1.4	Access	DPH	3 Contracted Syringe Services Program	No
Hepatitis Surveillance	Hepatitis C Virus	Surveillance	Acute and Chronic Hepatitis C Virus	CTEDSS	Proprietary	DPH	DPH	Yes
Immunization	Hepatitis B Virus	Surveillance/ Prevention Case management	Acute , Chronic and Perinatal Hepatitis B virus	CTEDDS	Proprietary	DPH	DPH	Yes
Immunization	Registry	Surveillance	Immunization Registry	CIRTS	Proprietary	DPH	DPH	Yes

# Appendix H

## 2014 Reports of Reportable Diseases

DISEASE	Total
Anthrax	0
Babesiosis	170
Botulism (includes infant)	0
Brucellosis	0
California group virus	0
Campylobacter	811
Chikungunya	35
Cholera	0
Cryptosporidiosis	43
Cyclospora infection	8
Dengue Fever (confirmed & probable)	4
Diphtheria	0
Eastern Equine Encephalitis (human)	0
<i>Escherichia coli</i> O157:H7 gastroenteritis	17
<i>Escherichia coli</i> non-O157, Shiga-toxin producing	42
Giardiasis	209
Group A streptococcal disease, invasive	140
Group B streptococcal disease, invasive	435
<i>H. influenzae</i> type B disease, invasive	4
<i>H. influenzae</i> disease, invasive, other serotypes	56
Hansen's disease (Leprosy)	0
Hemolytic-uremic syndrome	5
Hepatitis A	23
Hepatitis B (acute)	9
Hepatitis B (chronic)	NA
Hepatitis C (acute)	0
Hepatitis C (chronic/resolved)	2,410
Human Granulocytic Anaplasmosis*	76
Human Monocytic Ehrlichiosis	0
HIV	273
Influenza associated deaths, all ages	45
Legionnaires disease	59
Listeriosis	14
Lyme disease (confirmed)	1,675
Lyme disease (probable)	624
Malaria	16
Measles	5
Meningococcal disease	2
Mumps	3
Neonatal sepsis	17
Pertussis (confirmed and probable)	100
Plague	0
Pneumococcal disease, invasive	237
Poliomyelitis	0
Q Fever	0
Rabies (human)	0
Rabies (animal)	183

<b>DISEASE</b>	<b>Total</b>
Rocky Mountain Spotted Fever	0
Rotavirus	69
Rubella	0
Salmonellosis	463
<b><i>Sexually Transmitted Diseases</i></b>	
<i>Chancroid</i>	0
<i>Chlamydia</i>	12,732
<i>Gonorrhea</i>	1,421
<i>Neonatal Herpes</i>	1
<i>Syphilis (&lt;1 year or early syphilis)</i>	136
Shigellosis	65
Staphylococcus Aureus, Methicillin-resistant, invasive	868
Tetanus	0
Trichinosis	0
Tuberculosis	60
Typhoid Fever	1
Varicella (confirmed & probable)	182
Vibrio infections	15
Yellow Fever	0
Yersiniosis	3
West Nile virus (fever & invasive)	6
Source: DPH	

# Appendix I

---

## Controlled Substances Drug Schedules\*

### **Schedule I Controlled Substances**

Substances in this schedule have no currently accepted medical use in the United States, a lack of accepted safety for use under medical supervision, and a high potential for abuse.

*Some examples of substances listed in Schedule I are: heroin, lysergic acid diethylamide (LSD), and 3,4-methylenedioxymethamphetamine ("Ecstasy").*

### **Schedule II/IIN Controlled Substances (2/2N)**

Substances in this schedule have a high potential for abuse which may lead to severe psychological or physical dependence.

*Examples of Schedule II narcotics include: meperidine (Demerol®), oxycodone (OxyContin®), Percocet®, morphine, opium, codeine, and hydrocodone.*

*Examples of Schedule IIN stimulants include: amphetamine (Dexedrine®, Adderall®), methamphetamine (Desoxyn®), and methylphenidate (Ritalin®).*

### **Schedule III/IIIN Controlled Substances (3/3N)**

Substances in this schedule have a potential for abuse less than substances in Schedules I or II and abuse may lead to moderate or low physical dependence or high psychological dependence.

*Examples of Schedule III narcotics include: products containing not more than 90 milligrams of codeine per dosage unit (Tylenol with Codeine®), and buprenorphine (Suboxone®).*

*Examples of Schedule IIIN non-narcotics include: benzphetamine (Didrex®), phendimetrazine, ketamine, and anabolic steroids such as Depo®-Testosterone.*

### **Schedule IV Controlled Substances**

Substances in this schedule have a low potential for abuse relative to substances in Schedule III.

*Examples of Schedule IV substances include: alprazolam (Xanax®), clonazepam (Klonopin®), diazepam (Valium®), lorazepam (Ativan®).*

### **Schedule V Controlled Substances**

Substances in this schedule have a low potential for abuse relative to substances listed in Schedule IV and consist primarily of preparations containing limited quantities of certain narcotics.

*Examples of Schedule V substances include: cough preparations containing not more than 200 milligrams of codeine per 100 milliliters or per 100 grams (Robitussin AC®, Phenergan with Codeine®), and ezogabine.*

\*Schedule I drugs are considered the most dangerous class of drugs with a high potential for abuse and potentially severe psychological and/or physical dependence. As the drug schedule changes-- Schedule II, Schedule III, etc., so does the abuse potential-- Schedule V drugs represents the least potential for abuse.

Source: U.S. Department of Justice Drug Enforcement Administration (DEA)