Legislative Program Review and Investigations Committee
Connecticut General Assembly

Health Information Privacy in Selected State Programs

Staff Findings and Recommendations Report

December 16, 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. 2-53e) 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	***House***
John W. Fonfara, *Co-Chair*	Christie M. Carpino, *Co-Chair*
John A. Kissel	Mary M. Mushinsky
Eric D. Coleman	Whit Betts
Anthony Guglielmo	Henry Genga
Joe Markley	Philip Miller
Andrew Maynard	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

(860) 240-0300 www.cga.ct.gov/pri/index.htm PRI@cga.ct.gov

PRI Staff Findings and Recommendations Highlights

December 2015

Health Information Privacy in Selected State Programs

Background

In July 2015, the Legislative Program Review and Investigations Committee authorized a study to evaluate the management of personal health information, including certain confidentiality requirements, at the Department of Public Health's (DPH) Infectious Diseases Section (IDS) and the Department of Consumer Protection's (DCP) Prescription Monitoring Program (PMP).

IDS is responsible for collecting identifiable health data from across the state to assess infectious diseases and associated risk factors; identify and respond to emerging infections; and conduct outbreak investigations and surveillance. PMP maintains a statewide electronic database of dispensed prescriptions for controlled substances that allows prescribers to properly manage a patient's treatment, as well as to prevent the improper or illegal use of controlled substance prescription drugs.

Health information security and confidentiality is a multi-faceted concept, which requires a variety of safeguards and approaches to ensure proper management and implementation. By developing and implementing *administrative, physical,* and *technical* safeguards for both physical and electronic records, an agency can strengthen its capability to prevent security breaches, regularly monitor information usage and security, and react if an issue does occur.

To conduct this study, PRI staff: developed a data collection tool based on information security best practices and legal requirements to evaluate sufficiency of safeguards; interviewed various DPH and DCP staff, other state agency staff, and stakeholders; conducted literature searches; examined each agency's policies, procedures, and practices regarding safeguards; and evaluated the management and security of select databases.

Main Staff Findings

DPH and DCP need to build on existing *administrative* safeguards. Both agencies have a number of administrative policies and procedures in place to protect identifiable heath information; however, DCP does not have a specific employee confidentiality pledge, and DPH does not have comprehensive data breach policies. Neither agency has completed a risk analysis and risk management plan.

Both agencies have a number of *physical* safeguards in place to secure personal health information; however, gaps exist. Building protections have been established at both agency locations**.** Each agency has some policies and procedures to address the physical management of information, including information exchanged through mail, email, and faxes, but certain omissions should be examined.

Policies and procedures related to *technical* safeguards have been implemented but can be improved. Both agencies have protocols for assigning log-in credentials, downloading data, and the use of portable and external devices. While IDS staff are not allowed to download identifiable health data, that activity is not proactively tracked or restricted. Timely removal of inactive users from each agency's database and lack of regular auditing of databases for inappropriate activity were additional concerns. No breach of confidential data has been reported by either agency.

Each agency has established procedures for sharing information with authorized database users. Both DPH and DCP have permission-defined registration processes for regular database users with a number of security features and access controls.

DPH has a review process for the sharing of identifiable health information with researchers, though some enhancements are necessary. DCP lacks such a formal review process. DPH has an extensive review process of researchers' data requests and an agreement defining protective requirements; however, the requirements lack data breach protocols. DCP does not have a formal review process for research information requests or standardized confidentiality language within data sharing agreements. Neither agency verifies compliance with security provisions in written agreements.

PRI Staff Recommendations

Key recommendations for both DPH and DCP include:

1. **Conduct a comprehensive risk analysis and develop a risk plan** to assess the vulnerabilities to confidential data and formulate a plan to address identified risks;
2. **Perform periodic audits of server and database access** to check for any unusual or inappropriate activity that may compromise data security and integrity; and
3. **Strengthen controls over information shared with researchers** to ensure formal review processes and protections are in place for sensitive data.

Legislative Program Review and Investigations Committee Staff Office
State Capitol * 210 Capitol Avenue * Room 506 * Hartford, CT 06106-1591
P: (860) 240-0300 * F: (860) 240-0327 * E-mail: PRI@cga.ct.gov

Acronyms

ABCs	Active Bacterial Core Surveillance
ACLU	American Civil Liberties Union
BEST	Bureau of Enterprise Systems and Technology
CDC	Center for Disease Control and Prevention
COLLECT	Connecticut On-Line Law Enforcement Communications Teleprocessing
COOP	All Hazards Continuity of Operation Plan
CPMP	Connecticut Prescription Monitoring Program
CPMRS	Connecticut Prescription Monitoring and Reporting System
CTEDSS	Connecticut Electronic Disease Surveillance System
DAS	Department of Administrative Services
DCP	Department of Consumer Protection
DMHAS	Department of Mental Health and Addiction Services
DPH	Department of Public Health
EIP	Emerging Infections Program
FIPS	Federal Information Processing Standards
FOIA	Freedom of Information Act
HHS	Department of Health and Human Services
HIC	Human Investigation Committee
HIPAA	Health Insurance Portability and Accountability Act
IDS	Infectious Diseases Section
IRB	Institutional review board
ISMS	Information security management system
ISO	International Organization of Standardization
LHD	Local health departments
MOU	Memorandum of Understanding
NABP	National Association of Boards of Pharmacy
NAID	National Association for Information Destruction
NCSL	National Conference of State Legislators
NIST	National Institute of Standards and Technology
NNDSS	National Notifiable Diseases Surveillance System
OPM	Office of Policy and Management
OPRA	Office of the Public Records Administrator
PDA	Personal Data Act
PHI	Personal health information
PMP	Prescription Monitoring Program
PRI	Program Review and Investigations Committee
SmART	Small Agency Resource Team

LIST OF PROGRAM REVIEW COMMITTEE STAFF RECOMMENDATIONS

Policies and Procedures

1. **DCP should consider establishing a confidentiality pledge signed by DCP employees similar to the one used by DPH to ensure all employees are made aware of state agency confidentiality requirements.**

2. **Connecticut General Statutes Section 4-196 of the Personal Data Act should be amended to replace the current requirement to adopt regulations describing agency databases containing personal information with an annual database inventory conducted by the Office of Policy and Management. The resulting inventory of databases should be publically accessible, and should include information concerning the purpose of each database, categories of data stored in each database, how data are used, and categories of authorized database users.**

Risk Management

3. **DPH and DCP should update and/or correct inconsistencies in their all hazards Continuity of Operation Plans.**

4. **DPH and DCP should each perform a comprehensive risk assessment that focuses on the vulnerabilities of handling confidential information. As part of those assessments, both agencies should investigate using the BEST Threat and Vulnerability Analysis Team to provide a detailed analysis of the specific threats and vulnerabilities associated with each agency's information technology system's environment and configuration. The assessments should be used to develop comprehensive risk management plans for each agency.**

5. **DPH and DCP, in consultation with OPM, should develop comprehensive confidentiality breach policies and procedures that would establish criteria to: identify; track; assess severity of threat and information exposure; and make appropriate notifications to affected parties, if necessary, in the event of the unauthorized acquisition, access, use, or disclosure of confidential data.**

Appropriateness of Information Collected

6. **Both DPH and DCP should perform a data classification examination pursuant to BEST methodology. The examination should be performed in conjunction with a recent on-going OPM effort to inventory state databases.**

Physical Management of Information and Record Handling

7. **As part of a comprehensive risk analysis assessment, both DPH and DCP should evaluate the potential vulnerabilities that are currently represented by their respective policies and practices surrounding their handling of the physical and electronic flow of health information through the U.S. mail, fax machines, printing, email, and storage.**

Computer Access and Usage

8. **DPH and DCP should perform regular audits of computer records to check for inappropriate or unusual activity.**

9. **DPH should consider implementing procedures that would block or track staff downloads of identifiable health information to portable devices.**

Server Management

10. **Both DPH and DCP should perform periodic audits of server access to determine if there is any unusual or inappropriate activity.**

Database Security and Access Management

11. **Stronger procedures for the handling of inactive users at both DPH and DCP should be developed to ensure timely removal of unauthorized users.**

12. **Both DPH and DCP should perform periodic audits of database access activity to determine if there is any unusual or inappropriate activity.**

DPH Information Sharing

13. **For research proposals involving data sharing approved by DPH, the department should include within its written requirements researchers' responsibilities when there is a data breach.**

    At a minimum, DPH should require that researchers notify the department, as soon as practicable, of the discovery of any incident that involves an unauthorized acquisition, access, use, or disclosure of identifiable health information, even if the researcher believes the incident will not rise to the level of a breach. The researchers should provide a report detailing the severity of the breach, or suspected breach, including a plan to mitigate the effects of any breach and specifying the steps taken to ensure future breaches do not occur.

14. **When sharing identifiable health data, DPH should specify within its written requirements how that data should be destroyed, and develop a verification procedure, in addition to researcher attestation, to ensure all identifiable health data was destroyed upon study conclusion.**

15. **Within available resources, DPH should attempt to verify researchers' compliance with administrative, physical, and technical safeguard terms and conditions outlined in written agreements.**

DCP Information Sharing

16. **DCP should periodically conduct random audits of law enforcement use of active case numbers in the CPMRS system.**

17. **DCP should establish and implement written policies and procedures for the submission and approval of CPMRS information requests from public or private entities for research purposes.**

18. **DCP should develop standard language for written CPMRS/PMP information sharing agreements that address specific state confidentiality statutes, penalties for violations of any disclosure or misuse of information, and requestor responsibilities for data retention and destruction.**

19. **Within available resources, DCP should attempt to verify authorized CPMRS information receivers' compliance with administrative, physical, and technical safeguard terms and conditions outlined in written CPMRS/PMP agreements.**

Introduction

Health Information Privacy in Selected State Programs

In order to provide a wide range of public services, government agencies are required to collect and maintain personal information on citizens and businesses. This may include sensitive information such as home addresses, social security numbers, medical conditions, family relationships, biometric data, and personal finances. Properly protecting information privacy requires a multi-faceted approach that includes the management and monitoring of physical and electronic access to information.

Scope of Study

In July 2015, the Legislative Program Review and Investigations Committee (PRI) authorized a study to describe and evaluate how health information privacy is maintained in selected state agency programs. Specifically, the study was to review the management of personal health information, including certain confidentiality requirements, at the Department of Public Health's (DPH) Infectious Diseases Section (IDS) and the Department of Consumer Protection's (DCP) Prescription Monitoring Program (PMP). Specific areas of analysis were to include: a discussion of information privacy and its relationship to confidentiality; a description of current state and federal legal protections that relate to information privacy; the appropriateness of personal health information collected by IDS and PMP; and a review of the adequacy of program regulations, policies, and procedures for managing and protecting personal data. The complete study scope can be found in Appendix A.

Research Methods

An organization or agency that maintains personal data has an ethical, and often a legal, responsibility to maintain proper information security and confidentiality. Personal health information is considered particularly sensitive and is therefore protected by specific requirements and guidelines applicable to both private and public sector entities. In order to evaluate the adequacy of current information handling practices within Connecticut state agencies, program review committee staff created a data collection tool (found in Appendix B) based on best practices and legal requirements from across the information security sector. This tool consists of 65 primary questions that combine guidelines and standards from multiple sources, including the Health Insurance Portability and Accountability Act (HIPAA), the National Institute of Standards and Technology (NIST), the federal Center for Disease Control and Prevention (CDC), the International Organization for Standardization (ISO), and various state statutes and regulations. These sources are described further in Appendix C. The PRI data

collection tool was used to identify strengths and gaps within each agency's information management system.[1]

The program review committee staff employed several additional methods:

- *Interviews* – conducted numerous interviews with department staff, including program, information technology (IT), and human resources (HR) staff. In addition to interviews with DPH and DCP, interviews were conducted with staff from the Office of Policy and Management (OPM), Department of Administrative Services (DAS), Bureau of Enterprise Systems and Technology (BEST), and specialized IT staff of the State Auditors of Public Accounts. Interviews were also held with various IT professionals and interested stakeholders, including the Connecticut Pharmacists Association, Connecticut Association for Directors of Health, Connecticut State Medical Society, American Civil Liberties Union of Connecticut (ACLU), and Connecticut Police Chiefs Association.

- *Literature research* – collected and reviewed relevant state and federal statutes and regulations addressing health information privacy. Committee staff also gathered literature, with the assistance of the National Conference of State Legislatures (NCSL), concerning information security industry standards and personal information handling in other states.

- *Document review* – examined documents provided by DPH and DCP, including policies, procedures, and practices concerning information security safeguards. Specific documents included staff handbooks, orientation materials, information security policies, Continuity of Operations Plans (COOP), and agency agreements and contracts. These documents were analyzed using the PRI data collection tool described above.

- *Process assessment* – evaluated the current management and security of select program databases, including the administrative, physical, and technical safeguards used by the departments and other responsible parties. The assessment included tours of relevant agency facilities.

- *Public hearing* – received testimony at a PRI public hearing held October 1, 2015.

[1] The data collection tool created for this study provides an overarching evaluation of an agency's data handling policies and procedures. It is meant to provide basic information and focus further areas of research, but does not serve as a risk assessment or formal evaluation.

Limitations

The scope of this study did not include an overall performance evaluation of the selected state agency programs. In addition, due to the time constraints faced by the 2015 study cycle, the findings and recommendations in this report are based only on the information and documents provided by the departments and stakeholders. The methods used in this study did not include testing or direct examination of the performance or functionality of electronic or physical access controls, security configurations, incidence response capabilities, or back-up operations.

Report Organization

This report is organized into three chapters. Chapter I contains an overview of the concepts of personal data and confidentiality within health care, and relevant state and federal laws concerning information privacy. It also describes the basic structure and operation of DPH's Infectious Disease Section and DCP's Prescription Monitoring Program. Chapter II discusses the results of committee staff's review of current information security safeguards, using the PRI data collection tool as a framework. Chapter III provides details concerning the information sharing procedures of each department's program and the adequacy of these procedures. Chapters II and III both contain committee staff's findings, as well as recommendations for improving protection of personal data.

Chapter I

Overview

This chapter provides necessary contextual and background information for the findings and recommendations of this study. Topics include a basic definition of personal information, the importance of confidentiality within health care, a brief overview of relevant laws and regulations, and general descriptions of the Department of Public Health's (DPH) Infectious Diseases Section (IDS) and Department of Consumer Protection's (DCP) Prescription Monitoring Program (PMP).

Personal Information and Privacy

Definition of personal information. Personal information, or personally identifiable information, is a concept discussed in many fields and sectors. While specific definitions vary by source and context, the core characteristic that makes data or information *personal* is if it can be classified as *identifiable*. If any variables, either independently or in conjunction with other available variables, can be used to identify an individual person, then the information is considered identifiable.

The Connecticut Personal Data Act (PDA) defines personal data 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."[2] The analysis conducted in this report refers specifically to personal health information, which is generally defined as any health information that can be attributed to a specific individual. Both general personal information and personal health information are protected in many contexts by both federal and state requirements.

Confidentiality in health care. The collection and use of personal health information has societal benefits, in the form of health research, public health activities, and health care oversight, as well as individual benefits, including access to more efficient and effective coordinated health care services.

While there are justifiable benefits, there are also significant risks associated with the collection, use, and sharing of personal health information. Privacy and confidentiality are tenets within the health care field intended, in part, to create a trusting environment within the patient-provider relationship. Due to the sensitive and sometimes stigmatizing nature of health information, a trusting environment is essential to increase the likelihood that patients will feel comfortable sharing their medical history and current concerns with providers. This confidentiality and privacy applies not only to the providers themselves, but also extends to the

[2] C.G.S. Sec. 4-190(9).

maintenance or transmission of personal health information for any reason, including public health reporting, billing purposes, and medical referrals.

Health information security and confidentiality is a multi-faceted concept, which requires a variety of safeguards and approaches to ensure proper management and implementation. Three overarching concepts within the health information security sector are:

- *confidentiality* – information is accessible only by authorized individuals and processes;
- *integrity* – information is not altered or destroyed in an unauthorized manner; and
- *availability* – information can be accessed as needed by authorized individuals.[3]

When describing health information handling, the federal Department of Health and Human Services states that "security is not a one-time project, but rather an on-going, dynamic process that will create new challenges as organizations and technologies change."[4] Public agencies, as well as health care providers, are responsible for ensuring the ongoing security and confidentiality of personal health information.

Department record confidentiality. Due to the sensitive nature of the personal health information collected by the Infectious Disease Section of DPH and the Prescription Monitoring Program of DCP, all records collected, maintained, and used by both programs are considered "confidential" under Connecticut state law.[5] This confidentiality places strict limitations on the usage and release of program data, which can only be accessed for specific purposes and circumstances. While multiple federal and state laws, including those discussed in the next section, offer individuals the right to request access to their own personal records held by state agencies, these requests must be denied due to the confidentiality classification of IDS and PMP records.

Relevant Federal and State Laws

Multiple federal and state laws have been established in an effort to standardize the handling and security of personal information within a variety of contexts, including health care, education, business, and the public sector. While IDS and PMP are exempt from many of the provisions, a basic understanding of these laws helps frame any conversation about proper information management. The three laws discussed below are relevant to the handling and protection of personal data within the health care field and within state agencies in Connecticut.

Health Insurance Portability and Accountability Act (HIPAA). HIPAA is a 1996 federal law adopted 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 health

[3] Department of Health and Human Services. March 2007. Security Standards: Security 101 for Covered Entities. *HIPAA Security Series*, Volume 2 (Paper 1), p.3.
[4] Ibid.
[5] DPH record confidentiality - C.G.S. Sec. 19a-25 and DCP record confidentiality - C.G.S. Sec. 20-578.

care 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, health care clearinghouses, and health care providers.[6] HIPAA is often used as the precedent for the proper management of protected health information, even for those organizations and agencies that are not subject to HIPAA requirements.

> *Applicability to IDS and PMP*. As state 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.[7] Covered entities are able to share protected health information with DPH and DCP due to the public health provisions within HIPAA,[8] as well as Connecticut state law that mandates reporting practices.

Freedom of Information Act (FOIA). The Freedom of Information Act is a Connecticut state law passed in 1975, which "provides the public with rights of access to records and meetings of public agencies."[9] The primary intent of FOIA is to increase transparency and accountability of government entities. Under FOIA, members of the public are able to request access or copies of records maintained by public agencies, as well as attend public agency meetings. 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.[10]

> *Applicability to IDS and PMP*. Records collected and maintained by IDS and PMP are generally considered outside of, or excluded from, FOIA requests. First, records collected and maintained by IDS and PMP are classified as confidential within Connecticut statutes, and are therefore not subject to FOIA requests.[11] Second, even if this record confidentiality did not exist, FOIA excludes medical and personnel files, as well as any records pertaining to an ongoing public health investigation.[12]

Personal Data Act (PDA). 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 addresses areas such as staff training, reasonable precautions for the protection of personal data, and procedures to ensure individuals' access to their own personal data.[13]

---

[6] 45 C.F.R. §160.103.

[7] While DPH is classified as a *hybrid entity*, or an entity that performs both covered activities and exempt activities under HIPAA, the activities conducted by IDS are not covered under HIPAA protections. DCP and PMP do not qualify as covered entities under HIPAA.

[8] 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.

[9] FOIC, *Citizen's Guide*, (2008, Rev. 2011). Accessible at http://www.ct.gov/foi/cwp/view.asp?a=4161&q=488530

[10] The statutory confidentiality of IDS and PMP records excludes these records from release under FOIA. C.G.S. Sec. 1-210(b) contains provisions that exempt certain records from mandatory disclosure under FOIA.

[11] C.G.S. Sec. 19a-25 and C.G.S. Sec. 20-578.

[12] C.G.S. Sec. 1-210(b)(2) and C.G.S. Sec. 1-210(b)(16).

[13] Personal Data Act – C.G.S. Sec. 4-190 to 4-197.

Applicability to IDS and PMP. The confidentiality of IDS and PMP records limits the release of data from either program, including requests for personal data from individuals under PDA. While IDS and PMP are exempt from the information sharing portion of PDA, both programs are still required to uphold the remaining sections of the law, including staff training, minimum necessary information, information protection, and maintenance of up-to-date regulations.[14]

Department and program specific laws and regulations. Both IDS and PMP must comply with agency- and program-specific state statutes and regulations concerning the collection, maintenance, and use of personal data. These citations, along with additional relevant statewide statutes, regulations, and policies, are incorporated into the PRI data collection tool, described further in the *Research Methods* section of this report, and detailed in Appendix D.

Department of Public Health Infectious Diseases Section

The Connecticut Department of Public Health (DPH) is the lead state 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 health regulations and rules, educating communities, and providing grant funding and contracts for direct-service programming.

Reportable diseases. Among the most significant DPH responsibilities are infectious disease tracking and prevention of (or response to) epidemics. The public health commissioner is required by statute to update and publish an annual list of diseases and laboratory findings that certain health care providers and others must report to DPH, as well as to the local health director of the town in which the patient resides (i.e., reportable diseases). There are over 80 reportable diseases, each of which is classified by DPH into two categories.

- *Category 1* diseases, such as tuberculosis, measles, and foodborne outbreaks require that mandated reporters:
  - immediately report such findings to DPH by telephone on the day the disease is recognized or strongly suspected; and
  - mail or fax a written report, within 12 hours, containing additional information to DPH.

- *Category 2* diseases, such as Hepatitis C, human immunodeficiency virus (HIV), or influenza-associated deaths:
  - do not require telephone reporting; and
  - 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.

[14] Relevant sections of PDA were integrated into the PRI data collection tool. Additional details can be found in Appendix D.

Mandated reporters. 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 a reportable disease: health care providers, health care facilities, and others. Others include a variety of professions that interact with large groups of people, such as school and day care administrators, camp directors, and aircraft pilots. Most reports originate from physicians and clinical laboratories.

Infectious Diseases Section. The Infectious Diseases Section (IDS) of the department receives disease reports and 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. [15]

The Infectious Diseases Section is one of eight subdivisions of DPH. The section is further divided into four broad programs with about 100 employees collectively. The programs are:

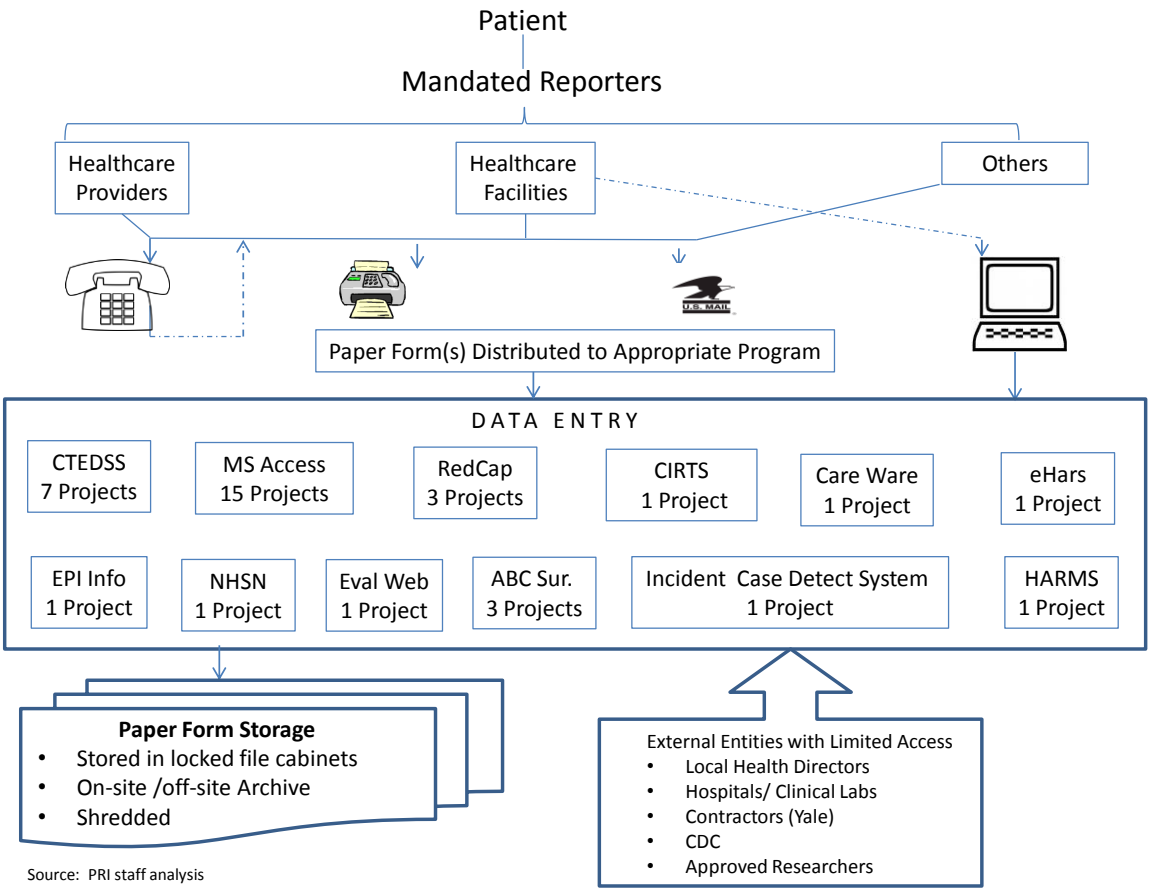
- Epidemiology and Emerging Infections;
- Immunizations;
- Healthcare Associated Infections; and
- Sexually Transmitted Diseases/HIV/Tuberculosis and Viral Hepatitis.

Information flow. Typically, IDS organizes its work by projects within program areas. Projects tend to be organized by disease or groups of diseases. Figure I-1 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, which will be detailed in the next chapter.

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.

[15] "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 21st Century*. MMWR 2012;61 (Suppl; July 27, 2012): p 3.

Figure I-1. Reportable Disease Information Flow



Source: PRI staff analysis

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 are particular to 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**. DPH receives reportable disease information through four primary modes: 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 uploading electronic files. As noted above, certain diseases require an immediate telephone response to 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 mandated reporters who call regarding patient care and remind them to fill out the appropriate form.

As will be discussed further, 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 regarding certain diseases.

3. **Data entry**. The information contained on the forms, including personal health data, is entered into one or more 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 which has thousands of records. Many of the small databases are for various research projects sponsored by the U.S. Centers for Disease Control and Prevention (CDC). Many database servers are located at and maintained by DPH. Others are located within the Department of Administrative Services' Bureau of Enterprise Systems and Technology (BEST), while others are located at the CDC and, in one case, with the City of Hartford.

4. **Paper form storage**. Thousands of paper forms are generated through this reporting process. In general, forms are kept for one year in 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.

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. This subject will be discussed in more detail in Chapter III.

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, a tuberculosis report requires an interview of the patient within three days to determine who came into contact with the infected person and evaluate 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 or her medication.

PRI selected databases. Because IDS has 28 databases that could not all be reviewed within the time frame of this study, PRI staff selected two databases used by the Connecticut Active Bacterial Core Surveillance (ABCs) project, which is housed within the Epidemiology and Emerging Infections program, for further review and evaluation. The ABCs project was selected because its databases have characteristics representative of many databases in IDS. These include:

- the project stores personal health information on two separate databases;
- one database is maintained by another agency;
- one of the databases is accessed through the Internet;

- there are a variety of internal and external users; and
- the personal health information security is not checked by another agency.

ABCs project description. The Active Bacterial Core Surveillance project is a key component of the Centers for Disease Control and Prevention's (CDC) Emerging Infections Program (EIP). The project is a collaborative effort among the CDC, Connecticut, and nine other states. Since 1995, the Connecticut DPH has been awarded federal funds via the CDC EIP cooperative agreement to conduct ABCs activities statewide.

The objectives of this project are to determine the incidence of and risk factors for invasive diseases caused by five bacterial pathogens: 1) Group A *Streptococcus*; 2) Group B *Streptococcus*; 3) *Haemophilus influenza*; 4) *Neisseria meningitidis*; and 5) *Streptococcus pneumoniae*. These bacteria can cause a wide range of infections. Some people carry these bacteria and have no symptoms of illness, while others develop invasive infections with severe and life-threatening consequences. Collectively, there were over 850 cases of these diseases confirmed last year in Connecticut.

Description of ABCs databases. The ABCs project stores identifiable health information on two databases. One of the databases is the Connecticut Electronic Disease Surveillance System (CTEDSS). The server on which CTEDSS resides is located in Groton. It is maintained by the Department of Administrative Services' Bureau of Enterprise Systems and Technology, which provides various information technology services to state agencies. This database stores information related to a number of reportable diseases in addition to the five that are covered by the ABCs project. The other ABCs database, called EpiInfo, resides on a server at DPH.

The data collected in CTEDSS contains core information about each ABCs case, including the patient's name, address, phone number, date of birth, sex, ethnic origin, race, type of disease, body site in which the bacteria was identified, and hospitalization information. These data are shared with certain staff at DPH, hospitals, and local health departments. These data are reported to CDC without the patient identifying information to satisfy certain federal reporting requirements through the Nationally Notifiable Disease Surveillance System (NNDSS).

In addition to the data in CTEDSS, the EpiInfo database contains answers to another two dozen or so questions providing additional details about the patient and the disease. These additional data elements must be collected by DPH as a recipient of CDC EIP funds. Data are used to monitor case trends, antimicrobial resistance of the bacteria, relevant molecular patterns, risk factors for the diseases, and effectiveness of prevention policies. The ABCs EpiInfo database provided by CDC is a data management system that is tailor-made to meet the needs of the ABCs project. It facilitates ease of collection and transmission of de-identified data to CDC. Although the CDC does not require EpiInfo be used as a separate database, the addition of specific ABCs modules within CTEDSS would require significant staff time and resources for development and ongoing maintenance. The ABCs EpiInfo database is provided free by CDC.

Additional details about the databases and the safeguards in place will be discussed in the next chapter.

Department of Consumer Protection's Prescription Monitoring Program (PMP)

The Prescription Monitoring Program (PMP) is housed organizationally within the Drug Control Division in the Department of Consumer Protection (DCP). The program is overseen by a division director and program supervisor. Since 2008, PMP has maintained a statewide electronic database of dispensed prescriptions for controlled substances, known as the Connecticut Prescription Monitoring and Reporting System (CPMRS). Prescription information for the PMP database is collected for schedules II, III, IV, and V controlled substances, as defined in state regulation.[16]

The database provides registered users a complete picture of a patient's controlled substance use, including prescription history from different providers. The information may assist 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 as well as to prevent the improper or illegal use of controlled substance prescription drugs.

CPMRS Management and Information Flow

There are two operating aspects of the CPMRS database: 1) data submission of reportable controlled substances to the system administrator, and 2) information access management handled by the program administrator. Since PMP's inception, the DCP commissioner has contracted with Optimum Technology, Inc. (Optimum), an out-of-state vendor, to be the system administrator, and electronically collect controlled substance prescription information in accordance with state laws governing pharmacies. DCP, as the program administrator, regulates the use of and access to the database.

System administrator. As system administrator, Optimum handles the information technology issues of uploading electronic submissions from the mandated reporters and identifying any data problems (e.g., conflicting, incomplete, or inaccurate data). As shown in Figure I-2, state law outlines who are mandated reporters and 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 data submissions are sent to the Optimum database server located in Ohio. Optimum also maintains a back-up server in Ohio, while a separate back-up server is located on-site at DCP. Once submissions are received, Optimum will identify any data problems and notify the mandated reporter to reconcile any data issues.

Program administration. DCP manages the CPMRS program administration including processing database registration applications, training, setting up user accounts, and handling access issues. Agency regulations indicate that the department must ensure patient information is

[16] Schedule I controlled substances are excluded from CPMRS because they 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.

collected, recorded, transmitted, and stored in accordance with applicable state and federal law, rules, and regulations.[17]

Access to database. All access to CPMRS is controlled by DCP. Dispensing 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. [18]

As illustrated in Figure I-2, practitioners in possession of a Connecticut Controlled Substance Registration[19] issued by DCP are required to register as a CPMRS user. Authorized practitioners include but are not limited to:

- medical doctors;
- pharmacists;
- dentists;
- veterinarians;
- advanced practice registered nurses; and
- physician assistants.

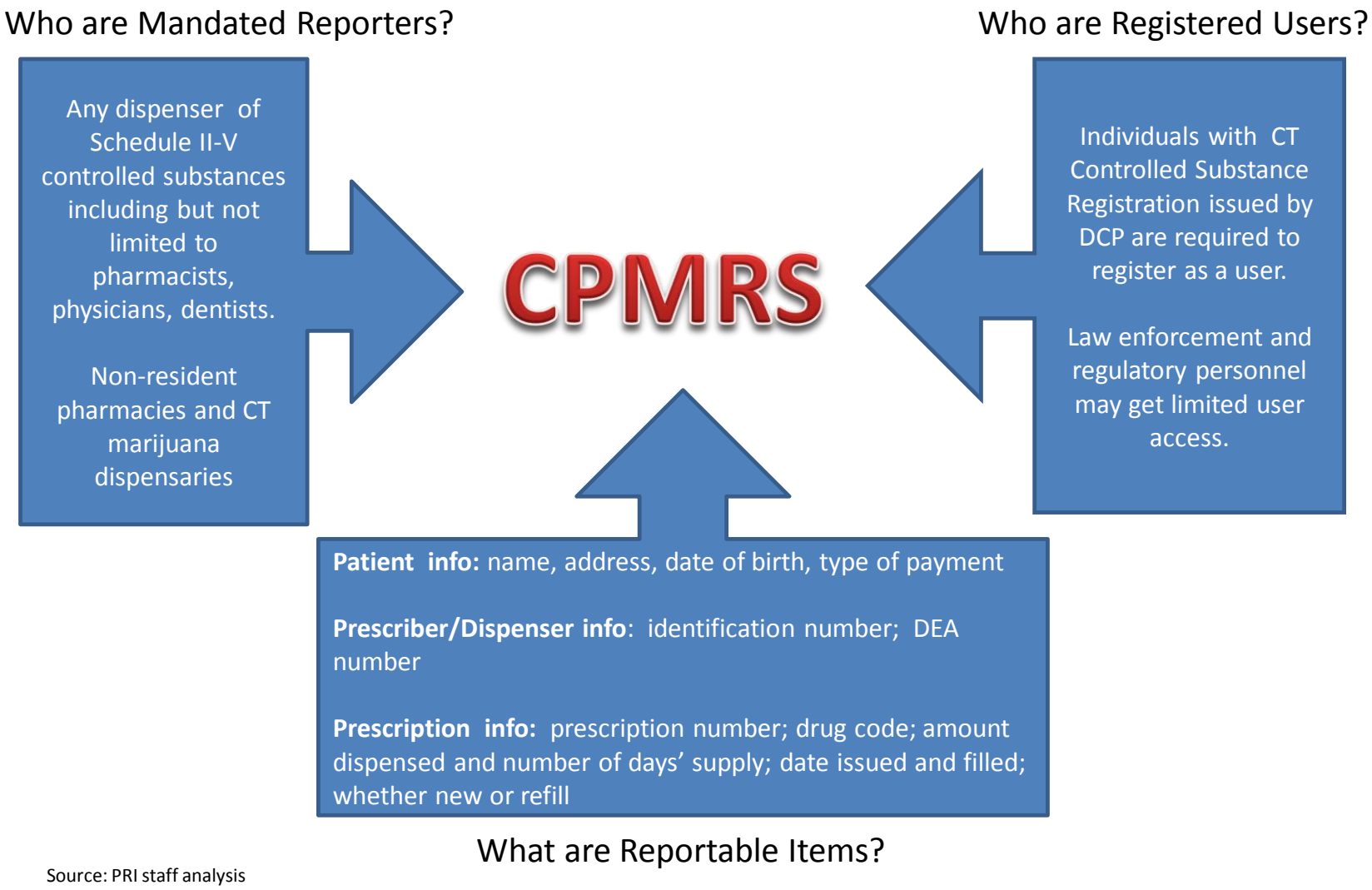
Limited access may also be granted to law enforcement and regulatory personnel. Further discussion on data access and information sharing is provided in Chapters II and III.

[17] Conn. Agency Regs. Sec. 21a-254-7.

[18] 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. (P.A. 15-198).

[19] This registration permits practitioners to distribute, dispense, conduct research, administer, or procure controlled substances in the course of their professional practice as permitted by the Department of Public Health or other governing agency.

Figure I-2. Connecticut Prescription Monitoring and Reporting System (CPMRS)



Source: PRI staff analysis

Chapter II

Evaluation of Safeguards

Within the field of information security, there are three overarching categories of safeguards that are considered best practice for agencies collecting, using, or maintaining personal data. By developing and implementing *administrative*, *physical*, and *technical* safeguards for both physical (paper) and electronic records, an agency can strengthen its capability to prevent security breaches, regularly monitor information usage and security, and react if an issue does occur.

As discussed earlier, PRI staff developed an assessment tool consisting of 65 questions that reference best practices and state statutory requirements for securing personal health information within each of the three categories of safeguards. PRI staff then compared PMP and ABCs project staff responses and department documentation to the criteria contained in the questions.

The following sections describe the three categories of safeguards, the sub-areas of each category, the definition and general criteria that can be used to evaluate the adequacy of these safeguards, the sufficiency of each department's current safeguards, and recommendations for how to strengthen health information protections.

Administrative Safeguards

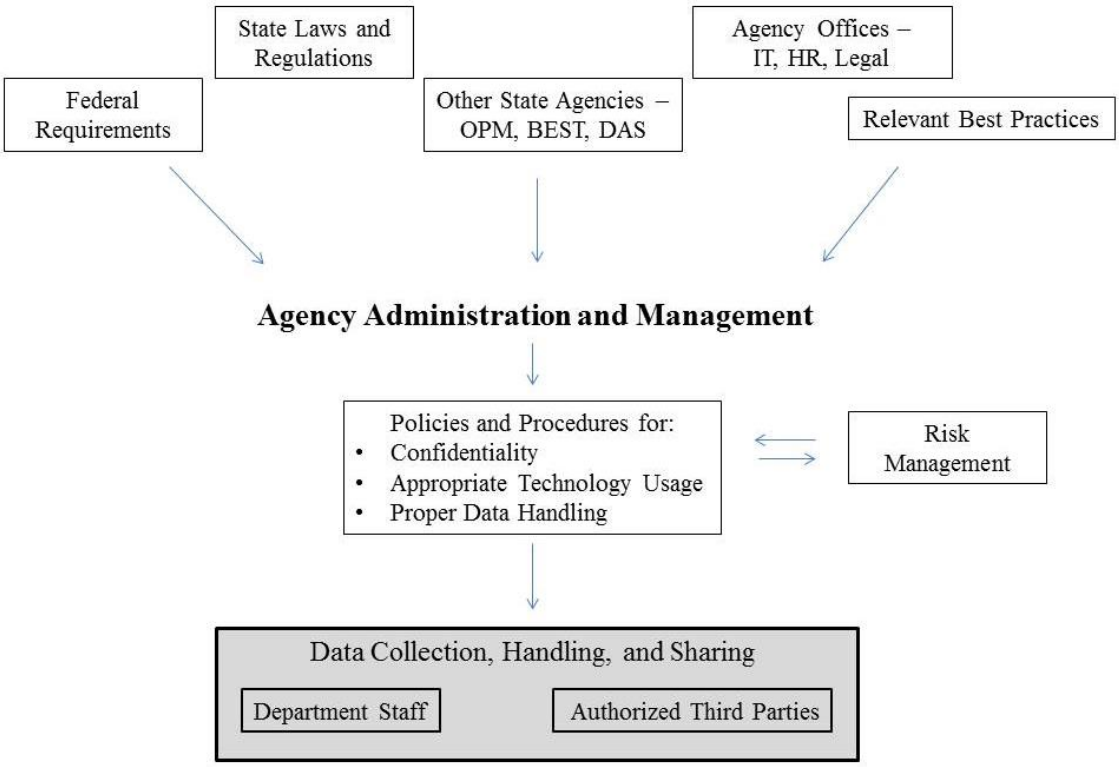
Administrative safeguards are "administrative actions, policies, and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected information and to manage the conduct of an agency's workforce in relation to the protection of that information."[20] The sub-areas of administrative safeguards are:

- formal policies and procedures;
- risk management; and
- appropriateness of information collection.

Figure II-1 provides a general conceptual overview of the formation and implementation process for agency policies and procedures concerning confidentiality, appropriate technology usage, and proper data handling. Specific policies and procedures are guided by a combination of factors, including federal requirements, state laws and regulations, policies from other state agencies, as well as specific administrative offices within an agency, and relevant industry best practices. Agency administration creates policies and procedures, informed by the agency's risk management plan, which are distributed to department staff and any authorized third parties who may handle agency data.

[20] Department of Health and Human Services. March 2007. Security Standards: Administrative Safeguards. *HIPAA Security Series*, Volume 2 (Paper 2), p. 2.

Figure II-1. Administrative Safeguards



Source: PRI staff analysis

Summary of findings. Based on the examination of administrative safeguards detailed below, PRI staff note that both DPH and DCP appear to have basic written policies and procedures related to the use of technology and the handling of confidential health information. But DCP, unlike DPH, does not have a specific employee confidentiality pledge related to identifiable health information.

Each agency has an all hazards Continuity of Operations Plan (COOP) to ensure agency operations can continue in the event of catastrophe, but lack a more comprehensive risk management plan. For the programs or projects reviewed, both agencies also appear to collect the minimally necessary information to accomplish their intended purpose consistent with state law. Neither agency has performed a data classification assessment of their databases as required by Bureau of Enterprise Systems and Technology. Finally, neither DCP nor DPH has experienced a breach of confidentiality policies in recent years.

ADMINISTRATIVE SAFEGUARD: Policies and Procedures

Definition

Formal and documented expectations, requirements, and processes that are intended to instruct and guide agency operations. Policies and procedures ensure consistency and accountability across an agency, and provide clear, specific instructions to all staff and management.

General Criteria

- All agency policies and procedures are:
  - Formal and written
  - Communicated to all staff, with training provided
  - Updated regularly
  - Monitored through a formal oversight process, including how to address violations and/or concerns
- Policies are inclusive of proper information security topics, including, but not limited to:
  - Confidentiality
  - Appropriate usage of technology
  - Proper data handling
- Updated agency regulations are maintained outlining:
  - General nature and purpose of the agency's personal data systems
  - Categories of personal and other data kept by the agency
  - Agency's procedures regarding the maintenance of personal data
  - Uses of personal data[21]

DPH policies and procedures. DPH has basic written policies and procedures regarding confidentiality, technology/equipment usage, and data handling. All policies are presented to department personnel at the start of their employment and are located (or electronic links are provided) in the DPH employee handbook. New employees acknowledge reading the handbook and agree to abide by department policies through signing a form. Confidentiality and record retention policy acknowledgements are signed separately. The confidentiality pledge specifically mentions the importance of and legal responsibility to maintain the confidentiality of personal health information collected by the department. It also states the confidentiality pledge applies throughout and subsequent to DPH employment.

The DPH Information Security Policy containing the technology/equipment usage and data handling policies was updated in August 2015. The Office of Policy and Management's acceptable use policy, which applies to all executive branch agencies and overlaps the DPH technology/equipment use policy, was promulgated in 2006.

The policies provided in the employee handbook establish a basis for imposing penalties. Violations may result in various disciplinary actions up to and including termination following a progressive disciplinary process. Staff are generally not required to re-sign these policies,

[21] C.G.S. Sec. 4-196.

though that practice is at the discretion of the human resources department. DPH reports that there have not been any violations of these policies within the ABCs project within the last three years.

DCP policies and procedures. DCP is part of the Small Agency Resource Team (SmART) established by the Department of Administrative Services (DAS) to combine several business office functions of various state agencies. The purpose is to encourage consistent application and execution of human resources rules and procedures as well as reliable interpretation. As such, new DCP employees are provided an orientation package of formal written policies and procedures regarding several topics including confidentiality, technology/equipment usage, and data handling that they must initial upon receipt. The package was last updated in May 2012.

The confidentiality provision contained within the state Code of Ethics policy broadly prohibits the use of confidential state information for financial gain.[22] There is no specific mention of personal health information as related to this study. PMP relies primarily on statutory language and agency regulations for operational guidance. In terms of information technology security, DCP staff recently received online training offered by SANS Institute, a vendor chosen by BEST, which aims to change information technology user behavior and helps organizations manage security risk.

Consequences for violations of PMP confidentiality and data handling requirements are outlined in statute. The Drug Control Division director indicates that he is responsible for communicating to his staff the consequences of any violations. Based on staff interviews, violations are only found if a problem arises or is brought to their attention. According to program staff management, violations would be handled on a case-by-case basis. The division director verbally explained the general process if a confidentiality violation was discovered (e.g., speak to employee to address concern, notify human resources, and involve the commissioner's office if necessary). To date, PMP program management states it has never had any violations pertaining to confidentiality or other policies or procedures.

DPH and DCP regulations. In addition to department and program-specific policies and procedures, agencies are required to maintain updated regulations concerning personal data management. The Personal Data Act required all state agencies to adopt regulations by January 1, 1978 that described:

- the general nature and purpose of the agency's personal data systems;
- the categories of personal and other data kept in the agency's personal data systems;
- the agency's procedures regarding the maintenance of personal data; and
- the uses to be made of the personal data maintained by the agency.[23]

[22] http://www.ct.gov/ethics/lib/ethics/publications/public_officials_guide_11.pdf
[23] C.G.S. Sec. 4-196.

Requiring agencies to publicly inventory information about their data systems increases transparency and awareness of how state agencies are using, handling, and protecting personal information. Both DPH and DCP are in compliance with the PDA requirement, as both departments adopted regulations describing their personal data systems by the 1978 deadline.[24] The most recent changes to the relevant IDS regulations occurred in 1995. Relevant DCP regulations were adopted in 1984, with the most recent update occurring in 2008 to the *Definitions* section. Regulations for both agencies contain out-of-date information and do not include many of the data systems currently used by DPH and DCP.

In order for these regulations to fulfill their purpose, they must be regularly updated to reflect changes and updates to agency data systems. However, regularly updating regulations might not be feasible because of the rate of technological change in state agencies.

In a more recent related effort, OPM is currently in the process of conducting a high-level database inventory to comply with Public Act 15-142. This act requires OPM to develop policies and procedures to protect and ensure the security, privacy, confidentiality, and administrative value of data collected by executive agencies. The inventory will identify whether data is considered to be protected (by law or regulation), sensitive, or public. The office will be using the information collected to better inform the development of the required policies and procedures. The maintenance of an updated database inventory, however, is not currently a requirement of the law. By formalizing a requirement that OPM maintain an updated public inventory of data systems, agencies will avoid the presence of obsolete data system information, thereby increasing accuracy and timeliness compared to the current reliance on agency regulations.

Key Staff Findings: Policies and Procedures

- Both DPH and DCP have basic written policies and procedures regarding confidentiality, technology/equipment usage, and data handling. However, DCP has relied primarily on statute and regulations for confidentiality provisions specific to health information.

- Unlike DPH, DCP does not require an employee confidentiality pledge related to personal health information.

- Neither DPH nor DCP have reported any violations pertaining to confidentiality within the last three years.

- Both DPH and DCP are complying with the Personal Data Act's required data system inventory. However, the current statutory language does not require regular updates to agency regulations concerning data systems that contain personal information. Consequently, the regulations have out-of-date and inaccurate information.

[24] Infectious disease epidemiology data system – Conn. Agency Regs. Sec. 19a-2a-12 and DCP data systems – Conn. Agency Regs. Sec. 21a-1-7a.

Staff Recommendations: Policies and Procedures

1. **DCP should consider establishing a confidentiality pledge signed by DCP employees similar to the one used by DPH to ensure all employees are made aware of state agency confidentiality requirements.**

2. **Connecticut General Statutes Section 4-196 of the Personal Data Act should be amended to replace the current requirement to adopt regulations describing agency databases containing personal information with an annual database inventory conducted by the Office of Policy and Management. The resulting inventory of databases should be publically accessible, and should include information concerning the purpose of each database, categories of data stored in each database, how data are used, and categories of authorized database users.**

ADMINISTRATIVE SAFEGUARD: Risk Management

Definition

Risk management encompasses both risk analysis and a risk management plan. A *risk analysis* is an "accurate and thorough assessment of the potential risks and vulnerabilities to confidentiality, integrity, and availability" of personal data.[25] The risk analysis should include the handling of physical (paper), as well as electronic, records containing personal health information. The results of this assessment are then used to formulate a *risk management plan*, which outlines the necessary security measures to reduce identified risks and vulnerabilities.

General Criteria

- Risk assessment is conducted regularly, to ensure that results are relevant and useful
- Risk management plan addresses topics including:
  - Security protocols and safeguards
  - Data back-up
  - Disaster recovery
  - Emergency mode operation
- Risk management plan is formal, documented, and distributed to appropriate agency staff
- Inventory of agency equipment, applications, databases, servers, and individuals entitled to access is maintained and updated[26]

[25] Department of Health and Human Services. March 2007. Security Standards: Administrative Safeguards. *HIPAA Security Series*, Volume 2 (Paper 2) p.4.
[26] C.G.S. Sec. 4-193(c) and Conn. Agency Regs. Sec. 19a-2a-23.

DPH risk management. The department has data back-up, disaster recovery, and emergency operation plans. The disaster recovery and emergency operations plans are contained within the department's all hazards Continuity of Operations Plan (COOP). The current version was created in August 2014 and reviewed and updated in January 2015. The COOP provides guidance to agency personnel to ensure that essential agency operations can continue in the event of a catastrophe.

Program review staff noted that in the portion of the plan listing the agency's essential functions and records by organizational unit, the information technology (IT) unit contained 23 databases that were not characterized. The characterizations are used to classify how critical the databases are to the operation of DPH and describe other important information, such as the existence of another copy of the database and if the database is connected to the Internet (which may be able to be accessed remotely in an emergency). These are important considerations in emergency planning.

In addition, the CTEDSS database was characterized differently by the IT unit and the Infectious Diseases Section. Specifically, the database's degree of importance and its connection to the Internet were inconsistent.

The only risk assessments performed at DPH have been narrowly focused on HIPAA compliance. The former state Department of Information Technology received funding from OPM to perform a HIPAA risk assessment for several state agencies, including DPH. One round of assessments was performed in 2008, and another was completed in 2013. The department's public health lab is DPH's only area that is covered by HIPAA requirements. The department has not performed an overall risk assessment of threats and vulnerabilities concerning the handling of confidential health information.

Breach policies and procedures. DPH does not have *comprehensive* formal policies and procedures to respond to malicious, suspected, and/or accidental unauthorized acquisition, access, use or disclosure of confidential data or the information systems that support these data. The department does have specific policies and procedures for limited circumstances. These include:

- an incident reporting procedure for the loss of mobile computing devices (e.g., notebook computers, BlackBerry devices) and mobile storage devices (e.g., diskettes, magnetic tapes, external/removable hard drives, thumb drives); and

- breach of confidentiality procedures for the HIV/STD/TB/Hepatitis surveillance programs only, including the appointment of a confidentiality manager, requirement to investigate and document the nature of the breach, and possible notification of other parties (i.e., CDC, Office of the Attorney General) as necessary. This is federal requirement for these particular programs.

Comprehensive data breach procedures can help to mitigate the damaging effects of any breach incident. This includes appropriate notification to affected parties, if necessary, to

minimize any potential harm. In addition, security controls may be improved based on recognition and documentation of any realized threats and incidents.

Inventory. The department maintains and updates a regular inventory of physical electronic devices, software applications, and external information systems. All physical, software, and firmware additions to DPH networks are documented to preserve an audit trail for the current status of the data network.

DCP risk management. Similar to DPH, DCP has an all hazards Continuity of Operations Plan (COOP) for 2015. The PRI committee staff finds that the plan contains some of the essential risk management components. Interviews with BEST officials suggest that state agencies may request that BEST conduct an IT risk assessment. Currently, risk assessments are conducted upon request and when resources are available. Given limited resources, risk assessments are prioritized for state agencies receiving federal funding. According to BEST, DCP has not requested a risk assessment.

Breach policies and procedures. The system administrator for CPMRS, Optimum, has provided DCP with security documentation regarding what protections and processes have been implemented to identify the occurrence of and response to a cybersecurity event or disaster recovery. Protocols are in place for data breach notification to DCP. However, similar to DPH, there are no written policies and procedures for DCP's response to a data breach notification.

Inventory. PMP program management staff states that a physical inventory of devices, systems, software, applications, and external systems is performed annually by DAS.

Key Staff Findings: Risk Management

- Both agencies have an all hazards Continuity of Operations Plan containing some components of a risk management plan.

- The all hazards COOP in each agency revealed some inconsistencies (e.g., databases characterized differently) and/or were not fully updated (e.g., out-of-date back-up location).

- While the all hazard COOP is critical for continuity and succession, it is not a comprehensive risk management plan. A more developed risk management plan, informed by a risk assessment, would identify and address vulnerabilities to protected health information in any form (electronic or written) throughout its lifecycle.

- DPH and DCP do not have comprehensive breach policies and procedures to respond to the unauthorized acquisition of confidential data.

- Both DPH and DCP perform regular asset management inventories.

Staff Recommendations: Risk Management

3. **DPH and DCP should update and/or correct inconsistencies in their all hazards Continuity of Operation Plans.**

4. **DPH and DCP should each perform a comprehensive risk assessment that focuses on the vulnerabilities of handling confidential information. As part of those assessments, both agencies should investigate using the BEST Threat and Vulnerability Analysis Team to provide a detailed analysis of the specific threats and vulnerabilities associated with each agency's information technology system's environment and configuration. The assessments should be used to develop comprehensive risk management plans for each agency.**

5. **DPH and DCP, in consultation with OPM, should develop comprehensive confidentiality breach policies and procedures that would establish criteria to: identify; track; assess severity of threat and information exposure; and make appropriate notifications to affected parties, if necessary, in the event of the unauthorized acquisition, access, use, or disclosure of confidential data.**

ADMINISTRATIVE SAFEGUARD: Appropriateness of Information Collection

Definition

Personal data is defined in Connecticut statute 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."[27] Agencies are statutorily required to collect only the minimum amount of personal data possible to complete their identified task.

General Criteria

- Only minimally necessary personal data is collected, used, or maintained by the agency[28]
- Data fields are regularly evaluated for their necessity and relevance
- Current data classifications for each data field collected by the agency are maintained – Since 2010, each executive branch agency is required to determine the nature and sensitivity of any data for which it has custodial responsibility, following the Data Classification Methodology as developed and provided by DOIT (now BEST).[29] The purpose of data classification is to assist state agencies in appropriately recognizing the sensitivity of data and provide a baseline indication how of data should be protected.

[27] C.G.S. Sec. 4-190.
[28] C.G.S. Sec. 4-193(e). Many agencies, including DCP and DPH, have specific statutory and regulatory limitations concerning what specific data fields can be collected.
[29] *OPM Data Classification Policy*.

DPH appropriateness of information collected. The data fields used for the collection of information within the ABCs project are determined by both DPH and the Centers for Disease Control and Prevention. As described earlier, CTEDSS contains ABCs patient information required to be reported to DPH under physician and laboratory reporting requirements. Additional health information regarding ABCs pathogens is collected and entered into EpiInfo. The data elements for this program are evaluated on an as-needed basis by both DPH and CDC. Generally, the elements have been stable and have only been adjusted if there were changes in: 1) the epidemiology of the disease process; 2) testing methods; or 3) the definition of a case (to ensure uniform data collection).

At a minimum, state regulations authorize the department to gather the following patient information: first and last name; address; age and date of birth; race; sex; occupation; attending physician; and any behaviors that may have made the individual vulnerable to exposure.[30] Collection of the statutory minimum amount of patient information is necessary in order to enable the state to identify cases where immediate disease control is needed and for tracking morbidity and mortality over time.

PRI staff reviewed each of the data elements collected for the ABCs project. The data collected appears consistent with statutory requirements to collect only the minimum necessary and does not include extraneous information, such as social security number, occupation, or other unnecessary data. The department, however, has not performed a data classification review of their databases as required by BEST.

DCP appropriateness of information collected. Information collected for the CPMRS is dictated by state statute.[31] The data fields have not changed since inception and are the minimum required. Like other PMP programs throughout the country, the database fields are modeled on the standards of the American Society for Automation in Pharmacy. Data definitions are outlined in the CPMRS reporting manual that is distributed to all users. Similar to DPH, DCP has not performed a data classification review of their databases as required by BEST.

Key Staff Findings: Appropriateness of Information Collected

- Both DPH and DCP data collection practices appear to meet the "minimally necessary" requirement pursuant to state statute.

- Neither agency's data classification is BEST compliant.

Staff Recommendations: Appropriateness of Information Collected

6. **Both DPH and DCP should perform a data classification examination pursuant to BEST methodology. The examination should be performed in conjunction with a recent on-going OPM effort to inventory state databases.**

[30] Conn. Agency Regs. Sec. 19a-36-A4.
[31] C.G.S. Sec. 21a-254.

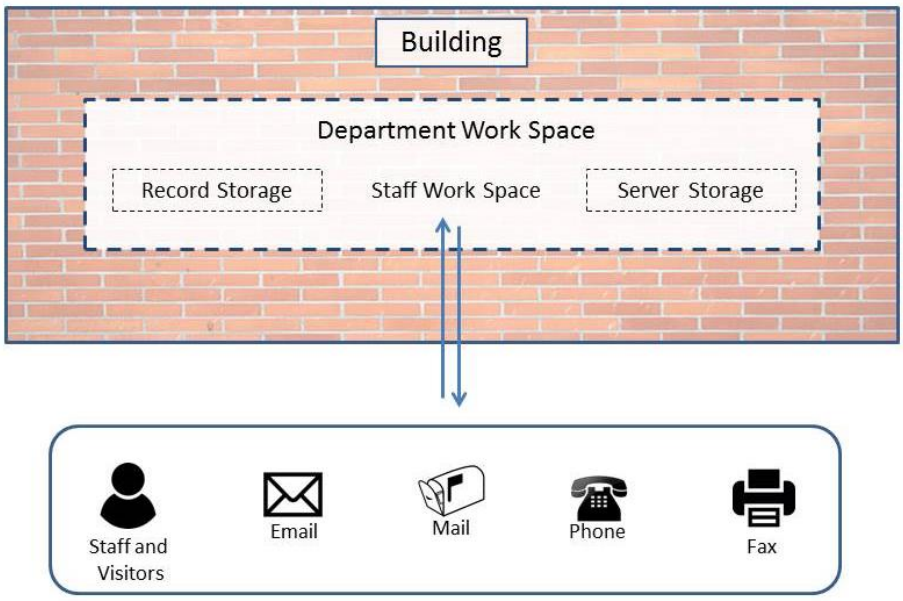
Physical Safeguards

Physical safeguards are "physical measures, policies, and procedures to protect information systems, related buildings, and equipment, from natural and environmental hazards, and unauthorized intrusion."[32] Physical safeguards can be divided into three sub-areas:

- building security;
- physical management of information; and
- record handling.

Figure II-2 illustrates the expected levels of physical safeguards present in agency buildings and workspaces. There are security measures required for both staff and visitors prior to entering agency buildings. Once in a building, there are safeguards that limit access to department workspace, record storage areas, and server storage areas. In addition to limiting access to physical spaces, agencies must also manage the physical movement of information, through mail, phone, fax, and email, into and out of department workspace.

Figure II-2. Physical Safeguards



Source: PRI staff analysis

[32] Department of Health and Human Services. March 2007. Security Standards: Physical Safeguards. *HIPAA Security Series*, Volume 2 (Paper 3) p.2.

Summary of findings. PRI staff finds that both agencies have a number of physical safeguards that assist in securing personal health information. However, some physical management of information policies and practices related to the handling of mail, fax, email, and printer security should be further assessed for vulnerabilities through a comprehensive risk analysis.

PHYSICAL SAFEGUARD: Building Security

Definition

Policies, procedures, and methods to limit physical access to information systems, as well as the facilities in which they are housed. Agencies are statutorily required to protect personal data from "fire, theft, flood, and natural disaster," as well as to limit physical access to only those staff that have programmatic need for the information.

General Criteria

- There are formal policies and procedures addressing:
  - Who has access to building and work areas
  - Process for granting and revoking physical access
  - Process for monitoring and auditing physical access
  - Process for granting and documenting visitor access to building and work areas
- Security methods and technologies to manage and monitor access, such as access control systems (badge access), cameras, security personnel, and methods to monitor visitor access.[33]

DPH building security. Building security safeguards at DPH appear to be in place. There are written policies and procedures that limit unauthorized physical access to personal health information including:

- photo ID badges for employees;
- visitor sign-ins with a security guard at the entrance;
- use of visitor escorts;
- locked entry to each floor;
- other departments are physically located on separate floors; and
- a requirement that employees physically secure information when away from their desks.

The workspace for the ABCs project is located within the IDS work area, which is a limited access area at DPH. The office space is a locked area that one must gain admittance into separately after signing in at the entry security station. Other IDS project staff and other DPH offices are co-located on the same floor.

[33] Conn. Agency Regs. Sec. 19a-2a-23.

DCP building security. The DAS Statewide Security Unit provides for the overall physical security of the State Office Building, the location for DCP. The DAS building security program includes conducting facility security audits, documenting recommendations for improvements, drafting security-related policies and procedures, purchasing and installing security equipment and systems such as access control, alarms, and video surveillance systems, and improving contract guard services. According to DAS, physical security standards pursuant to state law have been established.[34]

Various security practices are in place at the State Office Building where PMP workspace physically resides along with several other state entities. DCP employees are issued photo ID badges that must be shown prior to building entry. Badges also regulate access to areas within the building and use of certain office equipment. Visitors to the building must sign in and provide identification to an entrance security guard. There is no escort of visitors to offices. Information regarding an individual's physical access to the building can be tracked upon request. However, it was unclear how often access records are audited.

PMP workspace is located within the Drug Control Division, which is a contained work area separate from other agency divisions but where non-PMP staff has access to PMP staff workspace. PMP staff work alongside other Drug Control staff, which includes pharmaceutical investigators and staff for the medical marijuana program.

There is no written policy regarding securing physical copies of CPMRS data when PMP staff is away from their desks or during an emergency. PMP management staff believes this requirement is not applicable because the CPMRS is an electronic database. However, there is written policy requiring CPMRS users to lock computers when away from the workstation.

Key Staff Finding: Building Security

- Building security safeguards have been established at both DPH and DCP agency locations.

[34] C.G.S. section 4b-130.

PHYSICAL SAFEGUARD: Physical Management of Information

Definition

Personal data is collected, used, and maintained by agencies through a variety of methods and formats. These methods and formats include mail, fax, phone, print, and email. Management of this information includes policies, procedures, and methods addressing the definition, handling, and oversight of physical information within an agency.

General Criteria

- Policy specifies what methods are acceptable for transmission of protected information
- Procedures exist for the secure transmission of protected information, including specific requirements for:
  - Mail handling
  - Fax handling
  - Collecting and documenting information received over the phone
  - Printing of personal data
  - Email use
- Information access is limited to only those staff with programmatic need, using technologies and equipment such as:
  - Email encryption
  - Code-release printing
  - Secure fax machine (such as code-release fax, e-fax, or program-specific fax machines)
  - Secure mail handling area

DPH physical management of information. There are four primary modes through which DPH receives and handles information: mail, facsimile, telephone, and electronic.

DPH mail handling. A significant number of completed infectious disease report forms are delivered to the department by mail. There are no comprehensive and updated written policies and procedures for handling mail containing personal health information. Although there were limited mail handling procedures given to PRI staff that generally indicated which staff was to receive what mail, they were outdated.

The main mail room, where all DPH mail arrives, is secured by badge access and is limited to certain personnel. Program mail is distributed to DPH from the main mailroom to an unlocked program mailbox and is located in a common area for employees. In addition, staff mail boxes are in unlocked open containers, though the floor where the office is located is a limited access area.

DPH fax handling. In addition to mail, much of the reporting for infectious diseases comes from forms that are faxed to the department. There is a written policy that states DPH employees should only send the "minimum necessary" identifiable health information through a fax transmission. There is no requirement that faxes be retrieved in a timely manner by

department personnel. The ABCs project does not have a dedicated fax machine. The machine is located within a secured general office area of DPH but not in a locked room. There is a confidentiality disclaimer on all outgoing faxes.

DPH phone handling. The department will receive phone calls about reports of possible infectious diseases or suspected outbreaks from health care practitioners as well as the public. The most serious infectious diseases (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. A written report must be mailed or faxed to DPH within 12 hours.

The department's policy limits the sharing of personal health information over the phone to the "minimum necessary" amount to perform the intended task. Infectious disease staff will often enter information received over the phone directly into CTEDSS. However, staff will, at times, record certain information received over the phone into written notebooks, especially during off hours. The staff report that the notebooks are retained in a secure location but there is no policy that relates to the use, storage, or disposal of these notebooks.

DPH printing. The ABCs project has a shared printer that is located in the program's general work area. Staff do have a password protected printing option – that is, a document is printed only after an individual's password is entered using the printer's control panel. This function prevents unauthorized users seeing sensitive documents at the printer. The use of this function is currently optional. There is no specific written policy or procedure concerning the use of password protected printing of personal health information.

DPH email. Similar to its phone policy, the department has a general policy stating that emailed identifiable health information should be limited to the "minimum necessary" amount to perform the intended task. Emails are encrypted and a written procedure on how to securely send identifiable health information via email to non-state users has been developed by the DPH information technology division. The ABCs project and the larger epidemiology section has a more restrictive policy prohibiting the transmission of identifiable health information in emails; however, that policy is only verbally communicated to staff, not written. It is not clear how compliance with that policy checked or enforced.

DCP physical management of information. Recognizing that DCP's PMP is primarily an electronic program, policies regarding mail, fax, phone, email and paper records refer to any communications with registered database users that would not normally contain personal health information.

DCP mail handling. There is no separate written DCP policy for mail handling. However, procedures are followed that dictates who is responsible for receiving, sorting, and distributing mail. This includes a central mailroom that sorts and delivers to the individual offices within DCP. The mail room has checks for post-9/11 safety precautions. Once delivered to the Drug Control Division, administrative staff sorts and directly delivers mail to the appropriate recipient.

DCP fax handling. DCP has no written policy related to handling of faxes containing personal health information. DCP uses the RightFax system whereby faxes are directly sent to

the end-recipient via an email attachment. Each DCP worker has his or her own fax number. There is a conventional fax machine available in the commissioner's office for use, if necessary. There is a disclaimer included on all incoming and outgoing faxes.

DCP phone handling. There is no written phone usage policy addressing confidentiality of personal health information. PMP management staff state that this policy would not be applicable because personal health information is handled electronically and would not be discussed over the phone. However, there does not appear to be a phone usage policy for any other division activities such as investigations or the medical marijuana program.

DCP printing. DCP does not have written policy regarding printer usage for personal health information. PMP staff has a dedicated printer located in PMP staff workspace. Each staff has a unique printer code that releases print jobs via badge swipe.

DCP email. Although there is broad written policy governing the proper use of email (i.e., only for work-related purposes), there is no written policy guiding email handling of personal health information. PMP staff state that personal health information is never discussed via email. Department emails are encrypted according to BEST standards. The division director would be responsible for taking steps if any violations were discovered, as noted earlier.

PHYSICAL SAFEGUARD: Record Handling

Definition

Record handling generally includes record retention policies and procedures for physical (paper) and electronic records maintained by an agency. This includes how records are stored during use, when records are considered "inactive," methods for secure long-term storage, and proper methods for record destruction. Handling and retention policies and procedures ensure consistency, security, and accountability for all agency records, ensuring that access remains limited.

General Criteria

- All executive branch agencies are statutorily required to follow the Connecticut State Library's Office of Public Records Administrator record retention standards[35]
- Procedures include topics such as:
  - Records are to be kept under lock and key in both short- and long-term storage
  - Whenever possible, records are stored in a secure access area
  - Length of time a record is required to be retained
  - Proper destruction of both paper and electronic records
- Access to records is documented and auditable[36]
- Access to records is limited to only those staff who have specific need for access[37]

[35] Conn. Agency Regs. Sec. 19a-2a-12 and Conn. Agency Regs. Sec. 21a-326-3.
[36] C.G.S. Sec. 4-193(c) and Conn. Agency Regs. Sec. 19a-2a-23.

DPH record handling. The ABCs project is required to follow the official record retention schedule promulgated by the state's Office of the Public Records Administrator (OPRA), which requires that reportable disease forms be kept for a minimum of three years and reportable disease investigation files be kept for 10 years. The CDC does not have a specific timeframe for record retention but requires that program records be kept for as long as practical to allow for possible retrospective data collection and/or data cleaning. The ABCs project is in compliance with OPRA and keeps all project records for 10 years.

The department's data security policy states that physical documents with identifiable health information should be in an employee's possession at all times or stored in a secure location under lock and key. Within the ABCs project, the file cabinets have locks but keys cannot be located for all cabinets. Long-term storage of files is on site in a locked room. While general staff access to the locked long-term storage room is limited, the files are not kept in locked cabinets within the room. After 10 years, the files are shredded on-site by authorized DPH administrative staff.

DCP record handling. Similar to DPH, DCP follows the state record retention policy which dictates the length of time and storage location for documents from the Drug Control Division. State law requires the PMP program to maintain CPMRS records for a minimum of three years. According to PMP staff management, CPMRS records have been kept since the inception of the program in 2008.

PMP staff does not have locked cabinets and drawers but believes this practice is not essential to CPMRS operation because it is an electronic record. However, PMP documentation (e.g., compliance letters and registered user correspondence) is kept on-site.

DCP uses a private vendor, InfoShred, which is under state contract. InfoShred complies with all HIPAA requirements and is certified through an annual audit by the National Association for Information Destruction (NAID).[38] All InfoShred employees are required to sign a confidentiality agreement.

All DCP documents are shredded after the proper notice and approval from the Office of the Public Records Administrator. Upon completion of shredding and destruction services, InfoShred provides a Certificate of Destruction to verify that all confidential information was shredded.

Key Staff Findings: Physical Management of Information and Record Handling

- While both DPH and DCP appear to have some established policies and practices to address physical management of information (e.g., mail, phone, email, printer), additional enhancements should be considered. A risk

[37] Conn. Agency Regs. Sec. 19a-2a-23.

[38] NAID is a non-profit association that certifies destruction contractors through annual audits by independent security professionals. The audit includes review of company policy and document destruction procedure manuals, employment records, logs, and paperwork. It also examines facility security, monitoring systems, on-site and off-site destruction equipment, and access control systems.

assessment would assist in determining if the perceived risk or vulnerability is worth the cost of additional protections.

- Some improvements should be considered for the physical security of records at both agencies. For example, each agency indicated that file cabinets lack locks and keys.

Staff Recommendation: Physical Management of Information and Record Handling

7. **As part of a comprehensive risk analysis assessment, both DPH and DCP should evaluate the potential vulnerabilities that are currently represented by their respective policies and practices surrounding their handling of the physical and electronic flow of health information through the U.S. mail, fax machines, printing, email, and storage.**

Technical Safeguards

Technical safeguards are the "technology, and the policies and procedures for its use, which protects electronic protected information and controls access to it."[39] Exactly what technologies are utilized within each agency depends on the programmatic and administrative needs and capacity of each department.

While specific types of technology are dependent on the needs of an agency, it is recommended that any policies, procedures, or equipment concerning technology use are informed by the results of a risk assessment and compliant with a risk management plan. As with the administrative and physical safeguards, one of the primary goals of technical safeguards is to control and monitor access to protected information, and reduce the likelihood of unnecessary or unauthorized exposure of protected data. There are three technical safeguard sub-areas:

- computer access and usage;
- server management; and
- database security and access management.

As described in Table II-1, there are five overarching security safeguards essential to information security within an agency that collects, maintains, and/or uses personal information. These safeguards work to secure information that is stored and transmitted on agency computers, equipment, servers, and databases. They are often used to protect the integrity of *an entire network*, and are principal security methods that impact the three safeguard sub-areas described in this section.

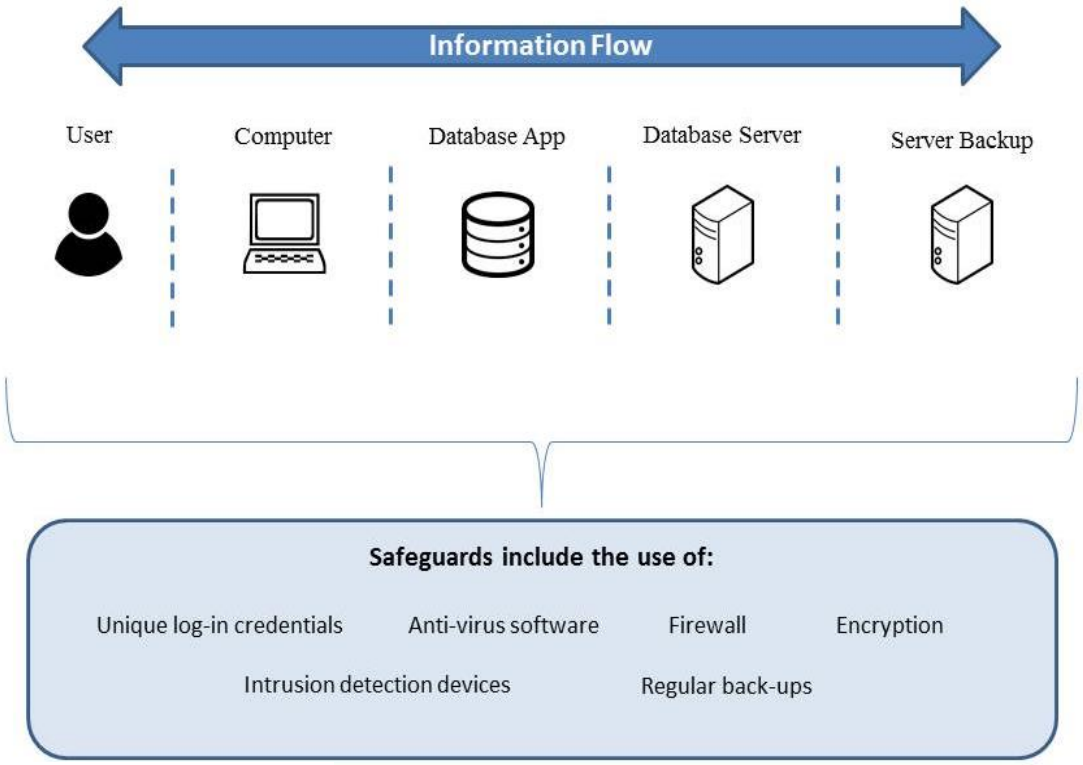
[39] Department of Health and Human Services. March 2007. Security Standards: Technical Safeguards. *HIPAA Security Series*, Volume 2 (Paper 4) p.2.

Table II-1. Description of Essential Technical Safeguards	
Firewall	A system designed to prevent unauthorized electronic access to or from a networked computer system. Firewall protection is generally used to secure Internet connections and transmissions.
Encryption	A method of converting electronic data into a form that can only be accessed by authorized parties. The primary purpose of encryption is to secure the confidentiality of digital data stored on computer systems or transmitted through the Internet or other types of computer networks. Any type of electronic information can be encrypted, including files, emails, and back-ups.
Anti-virus/intrusion detection software	Software that is designed to prevent, detect, and destroy computer viruses and other forms of electronic intrusion.
Data back-up	The practice and result of creating copies of electronic files and data for the purpose of being able to restore them in the case of data loss.
Least Access	A method based on the practice of granting users the minimum amount of access to systems and/or information necessary to complete their job basic function. This methodology applies to any limited access system, including access to agency computers, files, applications, and databases.

Source: PRI staff analysis

Figure II-3 shows a simplified scheme of the various levels of technical safeguards within a standard agency network. End users may be internal staff or authorized external users, with all users required to enter unique, role-based log-in credentials to gain access to agency computers and agency database applications. Any data entered or accessed through an agency database is stored on a database server, which is regularly backed up on an encrypted back-up server. Agency networks, including computers, databases, servers, and Internet connections, are protected using technologies such as firewalls, encryption software, anti-virus software, and intrusion detection devices.

Figure II-3. Technical Safeguards



Source: PRI staff analysis

Summary of findings. In general, from the analysis of technical safeguards described below, PRI staff note that both DPH and DCP have established policies and procedures for assigning log-in credentials, downloading, and the use of portable and external devices. While DPH does not allow the IDS staff to download personally identifiable health information, that activity is not proactively prevented or tracked.

DPH and DCP agency lacks procedures that ensure the timely removal of inactive users from their systems. Both agencies have the capability to, but do not regularly audit their databases and servers for any unusual or inappropriate activity. In addition, both agencies report they have not experienced a breach of confidential data in the last several years.

TECHNICAL SAFEGUARD: Computer Access and Usage

Definition

Computer access controls provide users with rights and/or privileges to access and perform functions using agency technology, applications, programs, and/or files. Proper computer access management ensures that electronic data are available only to those staff who have programmatic need for access, and protects data from loss, theft, or other inappropriate access. Access administration generally includes policies and procedures for permission levels (based on staff position), log-in credentials, inventories of agency assets and users, and access oversight and accountability methods.

General Criteria

- Policies and procedures include topics such as:
  - Limiting physical access to agency computers/equipment
  - Procedure for requesting, approving, and removing user access
  - Assignment of unique user credentials, including the use of strong passwords
  - Assignment of permissions based on *least access* methodology
  - Oversight and auditing of user access
  - Staff ability and authorization to use external storage or personal devices
  - Proper handling and protection of agency-approved portable devices (laptops)

- Agency computers/equipment are protected using:
  - Automatic lock or log-off functions
  - Encryption, firewall, and anti-virus software (described above)

DPH computer access and usage. Non-project staff have physical access to ABCs project computers but all employees are provided with individual log-in credentials with a requirement to change the password every 60 days. Formal procedures are in place to request, through an employee's supervisor, access to specific types of information that varies depending on staff responsibilities. (This procedure is explained further in the DPH database security section below.) All computers have encryption as well as anti-virus and anti-spam software which is updated daily.

Employees are required, by DPH policy, to lock or log out of their computers each time the computer is left unattended but this is not the default computer setting for ABCs project staff. All computers also have a password protected screensaver function to ensure that computers are left unsecured will be protected. Records are kept of staff log-in activity but this information is checked only if there is a request.

The official DPH policy allows identifiable health information to be transferred to external devices that are preloaded with DPH-approved password and encryption software. Staff are able to save files to their hard drives and to external devices (e.g., flash drive). Although the Infectious Diseases Section has a stricter policy in that it does not allow identifiable health information to be transferred to removable devices, there is no system blocking this ability or

tracking of this restriction. Employees are also given procedures on how security incidents, including lost, stolen, and vandalized laptops, must be reported.

DCP computer access and usage. Given the physical configuration of the DCP workspace, non-PMP staff has physical access to PMP computers. However, each DCP employee is provided individual workstation log-in credentials. Computers have password protected screensaver function. The department has a strong password policy that requires staff to change passwords every 90 days and prohibits the use of the same last ten passwords. The CPMRS policy and procedures manual requires users to lock computers prior to leaving their desk. Staff is able to save files on their computer hard drive or an external storage device. However, staff must only use state-issued equipment and resources. Department employees must adhere to state policy on the acceptable use of portable devices and/or personally-owned devices.

All agency computers have anti-virus software installed that is continually updated as updates become available. DCP uses encryption for Internet access as set by BEST. Records are kept of staff log-in activity. The department has the capability to review records for an indication of inappropriate or unusual activity. However, it is not clear how regularly reviews are done.

Key Staff Findings: Computer Access and Usage

- Both DPH and DCP have established computer access safeguards regarding log-in credentialing and policies for password protections, downloading, and use of portable and external devices.

- Although both agencies have audit capability, neither agency conducts regular audits of computer access activity.

- While DPH's Infectious Diseases Section has a strict policy of not allowing identifiable health information to be transferred to removable devices, there is no system blocking this ability or any tracking of whether this restriction is followed.

Staff Recommendations: Computer Access and Usage

8. **DPH and DCP should perform regular audits of computer records to check for inappropriate or unusual activity.**

9. **DPH should consider implementing procedures that would block or track staff downloads of identifiable health information to portable devices.**

TECHNICAL SAFEGUARD: Server Management
Definition A server is a computer/storage device that is designed primarily to provide shared access to data, and files. Most servers are connected to a network that enables authorized users/computers to access and retrieve stored data. Much like with physical (paper) files, the secure management of electronic files is essential to information security. Developing and implementing proper policies, procedures, and technologies helps to ensure that only those individuals who have authorization can gain access to personal data.
General Criteria • Policies and procedures include topics such as: – Physical security of servers – What types of information are authorized to be stored on servers – Procedure for requesting, approving, and removing user access – Assignment of permissions based on *least access* methodology – Records, oversight, and audits of user access[40] • Servers are protected using: – Storage of physical servers in secure, limited-access area – Encryption, firewall, regular back-ups, and anti-virus software (described above)

DPH server security (CTEDSS). As noted earlier, the ABCs project stores identifiable health information on two databases. The server on which CTEDSS resides is located in Groton and is maintained by BEST. EpiInfo resides on a server at DPH and is solely used for the ABCs project.

Because the CTEDSS server is Internet accessible, the entire system is protected by firewalls and intrusion prevention devices that blocks and detects unauthorized access. In addition, remote users do not have full access to certain servers from locations on the Internet to prevent misuse or corruption of the underlying data. BEST reports that there have not been any breaches of the firewall or intrusion detection devices that would have affected any DPH server. Each server has secure accounts for administration that are password protected and there is an event log recording details of who is accessing the server; however, it is not regularly reviewed.

The server operating system and security software is updated quarterly. The physical servers are kept in a secured area and access by staff is limited through ID badge verification. A record of who accessed the secured area is maintained. BEST staff must receive authorization by their division directors to obtain appropriate badge access. Vendors are escorted by state staff within BEST facilities. The CTEDSS servers are backed up nightly. On-site back-ups performed by BEST are not encrypted, but off-site back-up tapes are encrypted. BEST has contracted with

[40] C.G.S. Sec. 4-193(c) and Conn. Agency Regs. Sec. 19a-2a-23.

a secured disaster recovery facility in Springfield, Massachusetts, where off-site back-ups are stored.

DPH server security (EpiInfo). The server at DPH that contains the EpiInfo database is located in a physically secure room. Entry to the server room is obtained through a badge-based electronic access control system. DPH personnel access is limited based on the role they perform. A total of 22 DPH staff has access to the room. Cameras also monitor activity in the server room. While the system records information about who accessed the room and when, those records are only checked on request.

DPH servers are protected by anti-virus software that is updated bi-weekly. The servers are backed up incrementally on a daily basis and a full back-up is completed weekly. The department has security information event management software to detect any unauthorized intrusions.

DCP server security. As mentioned earlier, CPMRS servers are located in secure areas in both Ohio and on-site at DCP. Although the CPMRS database physically originates from the vendor's Ohio location, PMP stores a back-up version of the CPMRS database on its own server. This back-up can only be accessed by the program administrator. DCP reports that the server is password and firewall protected. BEST administers and monitors the firewall. The Drug Control Division director authorizes IT permission level for the PMP program administrator. There is one DCP/IT staff that has access to the server database. According to DCP/IT, the department can audit server access records up to one year and upon request.

The DCP server is physically located on-site in a secure area. DCP reports that ten individuals have authorized access to this area based on work necessity. Access audit records exist of who has entered the secure area. Servers are backed up on a nightly basis. According to DCP, the on-site back-ups are not encrypted as they never leave the secure area and are not accessible to external users.

Optimum server security. Optimum's data center has several layers of physical security including:

- unique coded key fob to enter the building;
- separate biometric hand print scanner with password to enter main and data center floor;
- key access to server cabinets as well as to access the server within the cabinets; and
- 24-hour audio and video surveillance of the data center.

Surveillance is reviewed weekly for suspicious activity or incidents that are not within the normal limits of business activity. Optimum also maintains HIPAA compliance by utilizing the following employment requirements: background checks, signed employment agreements to protect and secure sensitive patient data, and staff data security awareness training including what steps/measures should be followed if there is a security breach.

As noted previously, Optimum has provided DCP with security documentation regarding what protections and processes have been implemented to identify the occurrence of and response to a cybersecurity event or disaster recovery. According to the PMP program administrator, there have been no data breaches related to CPMRS to date. The database is encrypted and backed up daily.

Key Staff Finding: Server Management

- Server security safeguards for DPH and DCP appear to be in place.
- Although each agency has audit capability, checks for unusual or inappropriate activity on state servers is not regularly performed.

Staff Recommendation: Server Management

10. Both DPH and DCP should perform periodic audits of server access to determine if there is any unusual or inappropriate activity.

TECHNICAL SAFEGUARD: Database Security and Access Management

Definition

Many agencies use electronic databases to store, access, transmit, and analyze data and information. As with server security, database security and access management is necessary to ensure the protection and confidentiality of electronic agency data. Without proper policies, protocols, and methods, information can be vulnerable to inappropriate or unnecessary access, or from physical threats or theft.

General Criteria

- Policies and procedures include topics such as:
  - Procedure for requesting, approving, and removing user access
  - Assignment of unique user credentials, including the use of strong passwords
  - Assignment of permissions based on *least access* methodology
  - Training of users on proper use of database and confidentiality of data[41]
  - Oversight and auditing of user access and usage
- Database servers and applications are protected using:
  - Storage of physical servers in secure, limited-access area
  - Encryption, firewall, regular back-ups, and anti-virus software (described above)
  - Records and audits user access, record creation, record editing
- User access controls include:
  - Regular required password changes
  - Automatic account lock-out after failed log-in attempts
  - Automatic account lock-out after specified number of inactive days
  - Automatic log-out after specified number of inactive minutes

[41] C.G.S. Sec. 4-193(c), Conn. Agency Regs. Sec. 21a-1-7a, and Conn. Agency Regs. Sec. 19a-2a-23.

DPH database security and management (CTEDSS). There are six people authorized to grant access to CTEDSS and assign permission levels. They include the project coordinator, four field epidemiologists, and a health program associate. The field epidemiologists provide on-site assistance and training to hospitals and local health departments to set up user accounts. Each user is given a unique username and password. Passwords must be changed every 120 days. The database is backed-up nightly by BEST and off-site back-ups are maintained by a contractor in a secure facility in Springfield, Massachusetts.

The concept of least privilege is used to assign permission levels. In general, users are members of a group based on job responsibilities and disease specialization. There are four permission levels within CTEDSS – 1) super users; 2) extended users; 3) general users; and 4) limited users. The type of access that each category of user has and the number of users is noted in Table II-2.

Table II-2. CTEDSS Permission Levels

Type/Number of Users	Type of Access
Super 4 (DPH staff)	Global system access (highest permission level); access to all diseases in system; responsible for the management of the system; ability to view and update ABCs data and reports and workflow as part of development and maintenance responsibility.
Extended 2 (within ABCs project)	Create and view events; delete lab reports; run reports; modify workflows; reset passwords (DPH staff are limited by type of disease also).
General 1 (within ABCs project)	Add, view, delete, and modify select case information; assign and modify case status; close a case; and run reports
Limited 163 local health staff 58 hospital staff	Update questionnaires; manage attachments on records; run reports. Local health departments can only view cases in their jurisdiction. Hospitals can view and create cases for patients in their care. Limited users can add cases and/or edit case information; cases are not deleted once entered in the system but may be reclassified as 'not a case' or 'invalid case' by DPH staff.

Source: PRI created table based on DPH information

CTEDSS audit. The system has the capability to track the activity of users, but there is no written policy regarding reviewing or auditing system records for indications of inappropriate or unusual activity. The department would investigate any unusual activity brought to its attention. No concerns have been raised in the last three years over any unusual database activity.

The database does generate audit records regarding user access as well as record creation and editing. This information is kept indefinitely. The system also records user downloads but those records are only kept for two weeks. Policies and procedures for the use of audit tools have not been formalized.

CTEDSS inactive users. Although DPH policy indicates that inactive users will be removed if there is no log-in activity for 45 days, CTEDSS database users are only audited annually to discover inactive user accounts, which are then suspended. A new application will allow the project coordinator to set begin and end dates for temporary users but this does not address regular users outside of DPH or permanent employees who leave. Currently, ABCs project administrative staff are not in the DPH human resource notification system concerning staff changes, which could prevent the timely removal of staff who have terminated employment.

The database will automatically lock a user out after three unsuccessful attempts to gain entry. The database will also automatically log out a user after 10 minutes of inactivity.

DPH database security and management (EpiInfo). Although the EpiInfo database is now maintained by DPH, it was created by CDC, which is responsible for the underlying integrity of the database. The project does maintain a data dictionary of the data fields within EpiInfo. The database does generate audit records for user access including the date and time of access. Those records are retained indefinitely. When an employee leaves, notification is sent from human resources. There is a 60 day lock-out period if the user is inactive.

Although the EpiInfo database resides on a server, access to the database is configured so that it is only accessible through an application residing on authorized users' "C" drive. Thus, the protections discussed in the computer access section apply to EpiInfo.

There are only five DPH staff people who have access to EpiInfo, with no external users. There are no permission levels or limited users: a user either has full access or none. Access may be granted by two supervisory-level employees based on the role or job of the staff.

There are access audit tools but actual checking of employee access is done only upon request. There have been no formal concerns over database activity in the last three years.

DCP database security and management (CPMRS). The CPMRS database was initially created by DCP in conjunction with the vendor Optimum. Both DCP and Optimum currently oversee the technical maintenance of the database as the program and system administrators, respectively. As administrators, Optimum and PMP staff have access to the database.

New user accounts are set up by the PMP program administrator. Currently, there are over 20,000 registered users. Each user is given a unique username and a password that must be reset every 90 days. Registered users must also answer three security control questions.

Database permission levels for CPMRS user accounts are established by the PMP program administrator in accordance with the concept of least privilege. There are three

permission levels established for registered users: 1) prescribers; 2) pharmacists; and 3) law enforcement/regulatory officials.

Prescribers can view their own prescribing history and their patients but cannot view other practitioners' prescribing history or pharmacies' dispensing history. Similarly, pharmacists can look up their own dispensing history and their patients but cannot look up an individual practitioner's or other pharmacists' history. Law enforcement and regulatory officials may search for specific individuals if they have an active case number. However, approval is needed from the PMP program administrator to obtain any CPMRS report generated on prescriber or dispenser history.

The CPMRS data manual contains an access control policy that includes: the database purpose; scope of data collected; roles and responsibilities of users; compliance requirements; and audit and accountability tools. Training is provided to each registered CPMRS user prior to access being allowed.

CPMRS audit. The CPMRS system records the location, date, and time of database activity. According to PMP management staff, CPMRS can generate audit records of user access as well as record creation and editing. However, CPMRS does not allow downloads of data by anyone other than the program administrator. The CPMRS displays a notification on-screen stating actions are monitored for appropriate use and potential consequences for abuse of system.

There is no time limit to the availability of database activity records. Audits of individual registered user activity are possible but not regularly performed due to a lack of staff resources. In addition, auditing for potential account sharing is also impossible due to limited staff resources. The PMP program administrator does run CPMRS trend reports on a quarterly basis, which may indicate whether there is unusual activity. According to PMP program staff, the few times where an unexpected trend was noted, a reasonable and legitimate explanation was found.

*CPMRS inactive users***.** Only the PMP program administrator has the ability to remove inactive users as needed. Although the user registration agreement requires users to notify the program administrator of any name, facility, or job changes, there is no established protocol in place for this process. The program administrator must rely on the notification of changes from the users themselves as well as from the different professional oversight entities of the authorized user groups. About once a month, the PMP program administrator receives notices from other DCP division staff regarding a status change of a registered user's Substance Control Registration and from DPH regarding changes to the licensure status of health care practitioners. Occasionally, notices are received from law enforcement officials if there is personnel change for narcotic officers. At times, PMP staff becomes aware of a change when a new user registration is sought to replace a former user.

One technical safeguard to address this issue is the automatic renewal function for user registrations. The program administrator has set a three-year renewal limit. Once a user reaches the renewal date, the system will then prompt a user, upon attempt to log in, to update their registration information.

Other access security measures include: 1) inactive users are locked out of the system after 90 days; 2) users are automatically logged out of a session after 15 minutes of inactivity; 3) automatic lock-out after three unsuccessful log-in attempts; and 4) concurrent sign-in with a single username is not allowed.

Key Staff Findings: Database Security and Access Management

- Both DPH and DCP must strengthen procedures for the timely removal of inactive users.

- Neither agency regularly conducts audits of database activity to determine if there is any unusual or inappropriate activity.

- There have been no database breaches of DPH's CTEDSS or EpiInfo, or of DCP's CPMRS in the last three years.

Staff Recommendations: Database Security and Access Management

11. **Stronger procedures for the handling of inactive users at both DPH and DCP should be developed to ensure timely removal of unauthorized users.**

12. **Both DPH and DCP should perform periodic audits of database access activity to determine if there is any unusual or inappropriate activity.**

Chapter III

Information Sharing

Safeguarding privacy protections is critical to maintaining individuals' trust in their health care providers. At the same time, there are circumstances where health information may need to be shared to ensure the patient receives the best treatment and for other important public purposes, such as for the health and safety of the patient or others.

After the collection of specified data (as described in the previous chapters), both DPH and DCP may re-disclose that data to the extent allowed and in the manner prescribed by state and federal law. As shown in the table below, statutory safeguards should include delineating who is allowed to access the information, under what circumstances the information may be accessed, what criteria must be met for access, and for what purposes the lawfully accessed data may be used. Another crucial safeguard is clearly outlining the penalties for unlawful access and/or the unlawful disclosure of the data.

Information Sharing
Definition As the primary custodian of personal data, each agency is responsible for managing and limiting access to sensitive data, both inside and outside of the agency. Agencies may be authorized to share information, including personal data in some cases, with other entities for various purposes. They are also responsible for ensuring that any release of information is allowable by federal and state law, programmatically appropriate, and properly managed and secured.

General Criteria
 	
• Information is only shared for statutorily allowable purposes
• Formal policy, procedure, and criteria for evaluating and managing information requests
• Requests for information are submitted through written application, which includes:
  – Purpose
  – Requestor credentials and qualifications
  – How data will be used
  – How data will be secured
  – How information will be destroyed/returned when the project is complete
• Formal policy and procedure for the de-identification of data
• Approved releases require a written agreement describing the use, confidentiality, security, and destruction of provided data
• Formal oversight structure and process to ensure compliance with written agreements

Summary of findings. Each agency's information sharing practices adhere to the statutory requirements regarding allowable disclosure of data to authorized groups for specific purposes. DPH has implemented numerous comprehensive protections for information sharing regarding disease surveillance. DPH also has a well-established and formalized process for medical and scientific researchers, though some enhancements are necessary. Access to information within DCP's CPMRS is controlled through a permission-defined registration process for database users and the execution of written agreements for other statutorily authorized users. However, DCP lacks a formal review process with written criteria and protocols for data requests from public or private entities for research purposes.

The following section describes the information sharing allowed by both agencies including: each agency's legal authority to disclose data, each department's policies and procedures governing access to information, and specific findings and recommendations in these areas.

Department of Public Health

In order to fulfill its responsibilities to protect and improve Connecticut residents' health, DPH obtains a variety of confidential personal health information. The department receives requests from various organizations for data collected by many of its programs. In general, non-identifiable data, such as aggregated data and reports, are considered public documents and as such, are releasable.

The department may also allow certain individuals or organizations access to reportable disease information containing identifiable health information for specific reasons. Below is a discussion of the legal authority under which DPH can release personally identifiable health information, how access to the information is obtained, and the data protections that are in place.

Legal authority. By law, DPH is bound to protect and secure identifiable health information and is only authorized to release an individual's personal health information to:

- health care providers in a medical emergency to protect the health, life, or well-being of the person with a reportable disease;
- health care providers, local health directors, the department, another state or other public health agencies, or other persons when deemed necessary by the department for disease prevention and control;
- individuals, organizations, and government agencies for medical and scientific research;
- government agencies when conducting an audit, investigation, evaluation or investigation required by law; and
- perform its statutory and regulatory functions and to secure compliance with or enforcement of any laws.[42]

[42] C.G.S. Sec. 19a-25, Conn. Agency Regs. Secs. 19a-25-2 to 19a-25-4.

Data sharing for surveillance. As noted earlier, the department is responsible for collecting information about and responding to incidences of reportable diseases. Pathogen data related to the ABCs project is entered into CTEDSS and EpiInfo, which facilitates the collection of additional relevant information.

Access to the ABCs data (and other reportable disease data) contained in CTEDSS is granted to specific user groups to aid various aspects of disease surveillance, as noted in the table below.[43] In addition, selected protections, practices, or agreements involving confidential data are also indicated. In general, all personal information obtained through the department's disease prevention and control activities is required to be held confidentially and, by statute, any person who violates the confidentiality requirements can be subject to a $500 fine.[44]

Table III-1. Information Sharing of ABCs Disease Data for Surveillance

Agency	Purpose	Selected Protections/Agreements
Federal Government (CDC)	• DPH shares de-identified data with CDC for national aggregation and monitoring of diseases through the National Notifiable Diseases Surveillance System (NNDSS). • Public health officials use this information to monitor, control, and prevent the occurrence and spread of state-reportable and nationally notifiable infectious and noninfectious diseases and conditions.	• Data is de-identified. • Data is transferred using the Secure Access Management System, housed at the CDC, where each staff has unique and trackable sign-in credentials.
Local Health Departments/ Districts (LHDs)	• All ABCs pathogens are reportable to DPH and LHDs per statute. • LHDs have access to information and are responsible for certain follow-up activities that require access to CTEDSS.	• While there is no written user agreement, the department has a registration process that includes a written, signed confidentiality agreement. • There is an on-screen user pledge (visible when a user signs in to CTEDSS) to prevent unauthorized access and maintain data confidentiality. • LHDs are required to hold information confidential (Conn. Agency Reg. Sec. 19a-36-A5). • Obtain access through the Internet with individual log-in credentials. • LHDs are limited users: can only enter information in certain fields and only see records for patients under their jurisdiction.

[43] In general, other health care providers do not have access to CTEDSS.
[44] C.G.S. Sec. 19a-215(f).

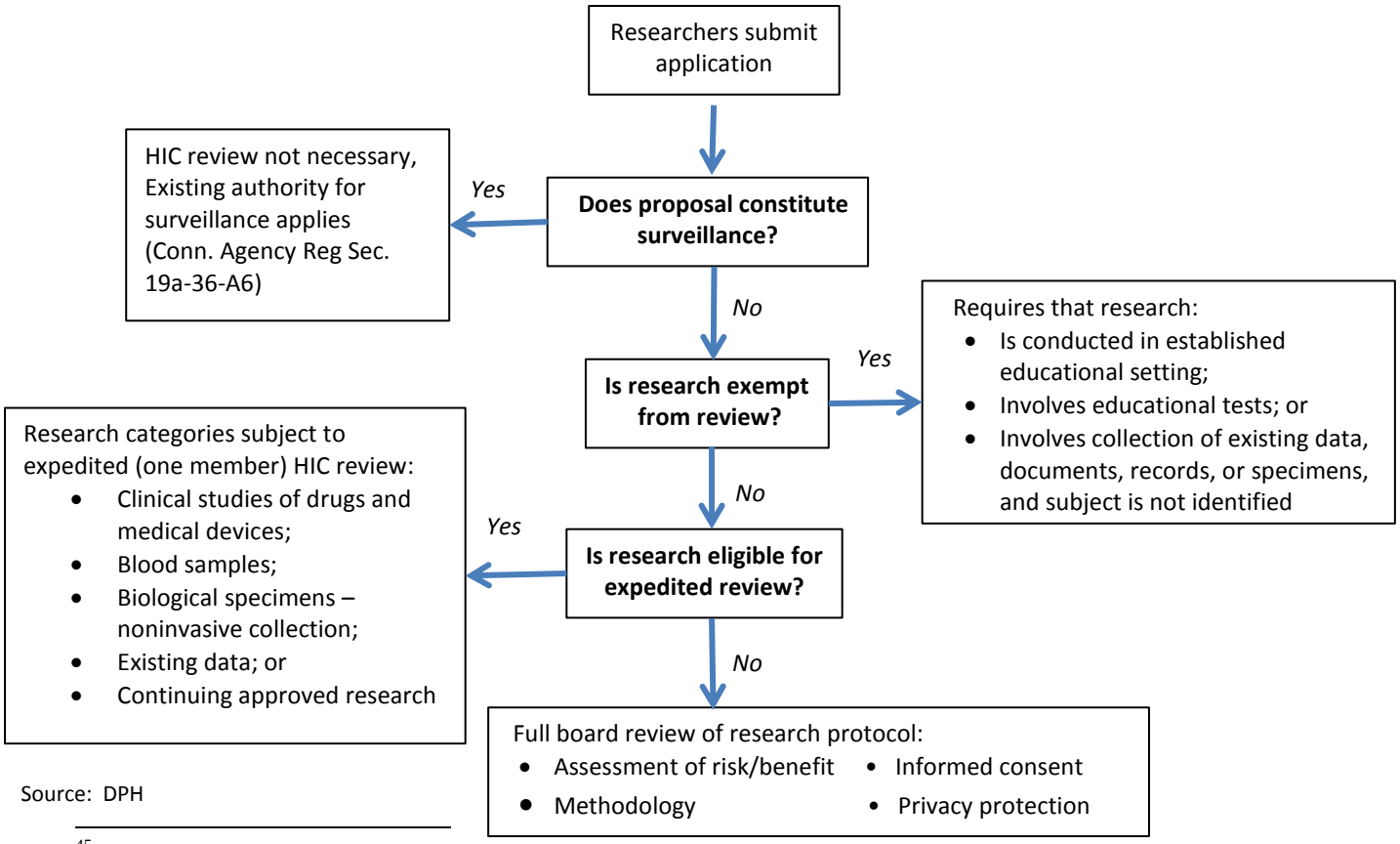
Table III-1. Information Sharing of ABCs Disease Data for Surveillance		
Agency	**Purpose**	**Selected Protections/Agreements**
Hospitals	• All ABCs pathogens are reportable diseases per statute. • Hospitals are required to report disease information; access to CTEDSS facilitates this reporting.	• While there is no written user agreement, the department has a registration process that includes a written, signed confidentiality agreement. • There is an on-screen user pledge (visible when a user signs in to CTEDSS) to prevent unauthorized access and maintain data confidentiality. • Hospitals are required to hold information confidential under HIPAA. • Obtain access through the Internet with individual log-in credentials. • Hospitals are limited users; can only enter information in certain fields and only see records for their own patients.
Contractors	• DPH hires temporary data entry personnel through a contractor to enter disease report information into CTEDSS.	• Obtain access through computers within the IDS work area. • Have individual log-in credentials. • Sign DPH confidentiality pledge.
Other DPH Employees/ Divisions	• Data is shared when two or more programs have statutory authority to obtain the same data and when implementing their legally authorized programmatic duties. • When the intended use of shared data is to conduct **research**, such requests for data must be submitted to the DPH Human Investigation Committee (HIC) for review and approval. (See below text for further explanation.)	• Department employees sign confidentiality pledge. • Department has a formal process requiring both sending and receiving section chief approval, adherence to agency-wide protocol, and official request form/documentation for data sharing. • A number of assurances must be agreed to regarding the handling and storage of confidential data.
Law Enforcement	• On rare occasions, reportable disease information may be shared with law enforcement for public safety reasons. • For example, in 2003, a case of cutaneous anthrax was diagnosed in a CT resident that prompted law enforcement follow-up. This (infection with *Bacillus anthracis*) was considered a potential bioterrorism-related event and therefore shared with law-	• A standard of sharing the minimum amount of information necessary for public health action is applied. • In the 2003 case, only relevant case information was provided (demographic and medical information about current infection).

	enforcement. This scenario would not apply to any of the ABCs pathogens as none are listed as bioterrorism agents.	• Only individual case information has been shared with law enforcement when appropriate. • Law enforcement access to CTEDSS has not been provided.

Source: PRI Interviews with DPH Staff

Data sharing for medical and scientific research. In addition to the user groups in Table III-1, DPH also releases identifiable health information to medical and public health researchers. In general, research is defined as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge."[45] Data collection for disease surveillance does not require review.[46] The department has established formal policies, procedures, and criteria to evaluate researchers' requests for identifiable health data. The review process is rigorous as outlined in Figure III-1.

Figure III-1. DPH Human Investigations Committee (HIC) Review Process



Source: DPH

[45] 45 C.F.R. 46.102(d).

[46] Surveillance means the continuing scrutiny of all aspects of occurrence and spread of a disease relating to effective control of that disease, which may include but not be limited to the collection and evaluation of: morbidity and mortality reports; laboratory reports of significant findings; special reports of field investigations of epidemics and individual cases; data concerning the availability, use, and untoward side effects of the substances used in disease control, such as rabies vaccine; and information regarding immunity levels in segments of the population. Conn. Agency Regs. Sec. 19a-36-A1.

Researchers must obtain approval from the department's Human Investigation Committee (HIC) before personal health information is released. The committee reviews research protocols to determine compliance with applicable federal and state law. The committee meets monthly and consists of not less than five voting members appointed by the public health commissioner. A chair and co-chair are also appointed by the commissioner. Minutes and decisions of the committee are maintained for all HIC meetings.

Research proposal. The application to HIC must contain: information about the principal investigator and other investigators; list of any other HIC or institutional review board (IRB) approvals; and the research proposal. The research proposal must include:

- an introduction to and a summary of the research proposal;
- research aims and goals;
- methodology, along with an explanation of and justification for obtaining DPH identifiable health data;
- description of measures to protect confidentiality;
- draft informed consent forms; and
- draft questionnaires.

Review process and criteria. As illustrated in the figure, after determining that the proposal is not public health surveillance, not exempt from review (for listed reasons), and ineligible for expedited review (for listed reasons), the full HIC reviews the proposal based on certain standards and criteria. These criteria include an examination of the proposal to ensure:

- risks to subjects are minimized;
- risks are reasonable in relation to anticipated benefits;
- selection of subjects is equitable;
- informed consent is sought from each subject and properly documented, if applicable;
- data collection is monitored to ensure subject safety; and
- privacy and confidentiality of subjects and data are protected.

The HIC committee's decision-making process uses an evaluation checklist with about two dozen questions related to the above criteria. The specific questions focus on the viability of the study goals, methods appropriateness, informed consent matters, research risk/benefit ratio, and researchers' qualifications.

Requests of information. Since January 1, 2012, 131 research proposals have been submitted to DPH overall. Ultimately, 63 were approved by the full committee, 26 received expedited review approval, 33 were found to be exempt from HIC approval, five were incomplete, two were rejected, and two were tabled. The ABCs project has had only one request in the last three years for information, which was approved. The researcher ultimately received de-identified information.

Assurances. If a research proposal is approved, the researchers are required to sign an "agreement to abide" document that outlines the researchers' duties relating to data protection and handling. The document explains that after approval has been granted, the department may terminate any study approval and request all DPH identifiable information be returned if the study is not conducted according to DPH requirements. After signing the agreement, the researcher agrees to:

- provide status reports of research progress;
- submit draft research manuscripts to HIC for review and approval -- which, in part, focuses on ensuring that no identifiable health data are included in the article;
- use the data only for DPH approved research;
- protect and not further disclose the data;
- deploy effective administrative, technical, and physical safeguards to protect the confidentiality of data and prevent authorized uses or access to it;
- establish a procedure for risk analysis to identify security violations;
- establish verification procedures for staff or other entities;
- create security measures to guard against unauthorized access to electronic identifiable health data transmitted by email;
- refrain from placing identifiable health data on personal computers, portable devises, and removable media unless the media are password-protected and encrypted;
- keep the identifiable health data at the principal investigator's institution under his or her purview; and
- require all persons working on the research, with access to DPH data, to sign a DPH-provided confidentiality pledge.

Two important pieces missing from the assurances required of researchers is an obligation to notify the department about a confidential data breach and a declaration that the data has been destroyed at the conclusion of the research. In the event of a breach, the department has stated the HIC would investigate the cause of the improper disclosure, examine the steps taken by the principal researcher to fix any violations, and determine whether the researcher would be required to destroy the data and stop the research.

De-identification. The HIC requires that researchers provide justification for requests for identifying health data. It is the committee's practice to approve the release of only the "minimally necessary" data to accomplish the research. The HIC follows the recognized HIPAA definition of data de-identification which includes removal of 18 types of identifiers.

Key Staff Findings: DPH Information Sharing

- DPH appears to have safeguards in place for electronic sharing of certain disease surveillance information.

- DPH generally has a comprehensive process for evaluating research proposals for the release of sensitive health data.

- DPH's "agreement to abide" includes many stipulations but does not: a) describe researcher responsibilities when there is a data breach; or b) require that the researcher indicate when data will be destroyed and the method of destruction, though researchers probably provide it in most cases, according to interviews with staff.

- DPH does not have a standard verification process to assure that the researcher has destroyed the data once the research project concludes.

- Other than researcher attestation, DPH does not independently verify administrative, physical, or technical safeguards employed by researchers with whom it shares data.

Staff Recommendations: DPH Information Sharing

13. **For research proposals involving data sharing approved by DPH, the department should include within its written requirements researchers' responsibilities when there is a data breach.**

    At a minimum, DPH should require that researchers notify the department, as soon as practicable, of the discovery of any incident that involves an unauthorized acquisition, access, use, or disclosure of identifiable health information, even if the researcher believes the incident will not rise to the level of a breach. The researchers should provide a report detailing the severity of the breach, or suspected breach, including a plan to mitigate the effects of any breach and specifying the steps taken to ensure future breaches do not occur.

14. **When sharing identifiable health data, DPH should specify within its written requirements how that data should be destroyed, and develop a verification procedure, in addition to researcher attestation, to ensure all identifiable health data was destroyed upon study conclusion.**

15. **Within available resources, DPH should attempt to verify researchers' compliance with administrative, physical, and technical safeguard terms and conditions outlined in written agreements.**

Department of Consumer Protection (DCP)

Access to information contained in the department's CPMRS is governed by statutory mandates, agency regulations, and written agreements (e.g., contracts, memoranda of understanding (MOUs)). As shown in Table III-2, DCP currently allows CPMRS data access by various groups for different purposes. A discussion of each is provided below.

Table III-2. Access to CPMRS

Type of User	Purpose	Allowed Through:
Registered Users:		
– Prescribers – Pharmacists – Law Enforcement	• Patient Care • Patient Care • Disciplinary, civil/criminal action	Registration
Public or Private Entities:		
– Researchers – Universities – State agencies	• Statistical, research, or educational purposes	MOU
Vendor:		
– Optimum	• System Administrator	Contract
Other States:		
– National Association of Boards of Pharmacy	• PMP Interconnect	MOU

Source: PRI staff analysis

Legal authority. State law establishes confidentiality protections for controlled substance prescription information in different statutory provisions. Connecticut General Statutes Section 20-578 establishes confidentiality for DCP's PMP records. The statutes also allow the DCP commissioner to contract with a vendor to electronically collect controlled substance prescription information for PMP in accordance with confidentiality laws.[47] In addition, agency regulations state that the department shall ensure patient privacy and confidentiality of patient information. Specifically, the agency regulations state DCP may provide PMP prescription information to:

- practitioners and pharmacists, for the purposes of patient care, drug therapy management and monitoring of controlled substances obtained by the patient;

[47] C.G.S. Sec. 21a-254(j)(5).

- other regulatory, investigative, or law enforcement agencies for disciplinary, civil or criminal action; and

- public or private entities, for statistical, research, or educational purposes provided the privacy of patients and confidentiality of patient information is not compromised.[48]

Registered CPMRS users. As noted previously, registered CPMRS users include prescribers, pharmacists, and law enforcement officials. User registration consists of a secure online application requiring basic contact information, profile information, (e.g., type of user, Drug Enforcement Agency (DEA) number, professional license number), and answers to three security questions. After receiving a DCP confirmation page, the registrant must print, review, and have the document notarized. As part of the required CPMRS registration, the registrants must fax the signed form along with a copy of their driver's license, passport or government issued photo identification. With the approved signed registration, the user receives a username with password and accepts the written registration policies and procedures for access to CPMRS. The policies and procedures document contains user responsibilities as well as user terms and conditions effective as of the date the user is registered.

Among the agreement's terms and conditions are to:

- comply with CPMRS policies, procedures, and standards;

- not permit unauthorized access to or use of the CPMRS application;

- safeguard CPMRS access by not disclosing or sharing user ID, password, and locking the computer when away from work area;

- immediately report suspected cases of misuse to the program administrator;

- notify the CPMRS administrator of any name, facility, or job changes; and

- only disseminate information for legitimate and official purposes consistent with all federal, state, and local laws.

As shown in Table III-3, the system safeguards allow users to make individual patient inquiries and to produce basic reports of their own prescribing/dispensing history based on the user's permission level.

[48] Conn. Agency Regs. Sec. 21a-254-6.

Table III-3. Authorized CPMRS Users		
Registered User (Number)*	**Purpose**	**CPMRS Protections**
Prescribers (16,964)	• for patient care, drug therapy management, and monitoring of controlled substances obtained by the patient	Only allows inquiries on patients and own prescribing history
Pharmacists (2,090)	• for patient care, drug therapy management, and monitoring of controlled substances obtained by the patient	Only allows inquiries on patients and own dispensing history
Law Enforcement (346)	• for disciplinary, civil, or criminal action	Only allows inquiries on patients with active law enforcement case investigation number. Request of PMP data for practitioner investigations must be discussed with PMP staff.
***As of November 2015**		
Source: PRI staff analysis		

The CPMRS also allows for three types of alerts when concerns are detected in the pattern of dispensing:

- prescribers may issue a 'person alert' when they have reason to suspect a patient of prescription drug abuse;
- pharmacists may issue a 'prescription alert' when they have reason to suspect that a prescription has been diverted (e.g., forgery, stolen prescription); and
- the system automatically generates 'patient threshold reports' for prescribers and pharmacists when some threshold of prescribers, pharmacies, or drug dispensed has been reached or exceeded by a patient during a given quarter.

The system is set up so that registered users can provide feedback or update the alerts. According to the CPMRS manual, policy and procedures violations may result in loss of CPMRS access and/or administrative or civil action against the user.

Law enforcement. To be an authorized CPMRS law enforcement user, an individual must be employed by a law enforcement agency or government agency authorized to review controlled substance prescriptions. The employee must hold a position that directly performs field work to obtain actual prescriptions and must also acquire approval from the Chief of Police

or principal drug control agent. There are 346 registered law enforcement users of CPMRS across state, federal, and local agencies.

The CPMRS information can only be used by on-duty officers on authorized department equipment for law enforcement purposes as part of an active case investigation. Under no circumstances can CPMRS be used for personal reasons or individual curiosity. CPMRS law enforcement inquiries cannot be used for background checks or pre-employment screening. A registered CPMRS law enforcement user may not request on behalf of another unauthorized agency or individual. Information obtained from CPMRS can only be shared with other law enforcement agencies in a joint, cooperative effort. Consequences for CPMRS misuse are clearly delineated in the written PMP policy as a computer crime pursuant to state laws.[49]

The written PMP law enforcement policy advises that CPMRS data should not be used as a substitute for original prescriptions located at pharmacies. Rather, CPMRS data should be viewed as an indicator of where the prescriptions are located. All information identified in the CPMRS must be verified by contacting the identified pharmacies.

The CPMRS system only allows law enforcement inquiries on patients with active case investigation number. Requests for practitioner investigations must be discussed with PMP management staff and/or the Department of Public Health's investigation unit for medical practice.

Access audit. As discussed in the previous section, the PMP program administrator runs trend reports on a quarterly basis and follows up on items that seem out of the ordinary. However, discussion with DCP staff suggests routine audits of specific CPMRS database usage are not done. Specifically, audits of law enforcement active case numbers are rarely done. PMP staff reports that it has, on occasion, prepared a list of active case numbers that is distributed to law enforcement supervisors to confirm whether the case number as active and assigned to the registered law enforcement users. The department contends that law enforcement officials are trained to adhere to privacy protections used in the Connecticut On-Line Law Enforcement Communications Teleprocessing (COLLECT) system and are aware of the gravity of policy violations of misuse of personal information.[50]

According to research by the National Alliance for Model State Drug Laws, 48 states and D.C. allow receipt of PMP information by law enforcement officials.[51] Of those, 30 states, including Connecticut, require that law enforcement officials have an active investigation with a case number in order to receive prescription monitoring information. Eighteen states require a search warrant, subpoena, or other judicial process before the information will be released.[52]

[49] C.G.S. Secs. 53a-251, 254, and 259(c) identify a computer crime in the third degree as a Class D felony and deems the value of private personal data to be $1,500.

[50] The COLLECT System is an online criminal justice system of intra- and interstate state and federal law enforcement resources. Access to COLLECT is granted only to law enforcement and criminal justice agencies.

[51] National Alliance for Model State Drug Laws (NAMSDL), *Annual Review of Prescription Monitoring Programs* (2015) p.2, Research current through September 2015.

[52] National Alliance for Model State Drug Laws (NAMSDL), *Annual Review of Prescription Monitoring Programs* (2015) p.22., Research current through September 2015.

Public and private entities. State regulations allow data disclosure to public and private entities for statistical, research, or educational purposes provided the privacy of patients and confidentiality of patient information is not compromised. There is no formal DCP process to evaluate the requests for CPMRS information from public or private entities. Generally, PMP management staff review these requests for information and decide on a case-by-case basis whether to approve each. If approved, the department and the requestor enter into a memorandum of understanding (MOU).[53] Since the program's inception in 2008, DCP has entered into a handful of MOUs to disclose PMP information to statutorily authorized individuals.

As seen in Table III-4, PMP has received six requests for CPMRS information. Three of the six were from university researchers; one was a joint research request from a university and a state agency; and two were from other Connecticut state agencies. As the table shows, three of the six requests were approved, two were denied, and one is pending. The table also lists the general study purpose, request outcome, and certain MOU requirements safeguarding personal identifiable information.

The three approved requests (Purdue, Brown, and DMHAS) had written agreements covering the terms and conditions whereby CPMRS data would be disclosed. Upon examination, the PRI committee staff found generally that the written agreements guiding the disclosure of CPMRS information for research purposes contained provisions for the use and confidentiality of personal health information. Two requests required PMP matching of patient names in order to link to another database. However, the data was de-identified once the linking was complete and before it was used by the researcher, pursuant to a protocol set out by the Department of Mental Health and Addiction Services (DMHAS). Two agreements addressed the disposal of information after the research project was completed.

State agency request. One of the requests was from the Department of Mental Health and Addiction Services (DMHAS) to comply with a statutory reporting mandate pursuant to C.G.S. Section 17a-451(o).[54] The MOU between DCP and DMHAS laid out the steps DMHAS research staff would perform by linking the data at the PMP offices, in the presence of PMP staff, using a matching algorithm previously developed and tested based upon "dummy" records provided by PMP staff. The MOU also stipulated that all transaction files would be destroyed in PMP staff's presence and the original personal identifying data set returned.

According to the MOU, use of the information would be in strict compliance with state and federal laws and regulations regarding patient confidentiality. The MOU specifically mentioned state and federal legal citations. As an additional safeguard, DCP written approval was required prior to publication or dissemination of any report based on the data.

[53] Generally speaking, a MOU is a formal document that expresses a mutual accord between two or more parties agreeing on an intended common line of action.

[54] The goal of linking the CPMRS with DMHAS' Substance Abuse Treatment Information System (SATIS) was to conduct a study on the individuals receiving substance abuse treatment for opiate abuse or dependence and the non-medical use of opiate prescription drugs prior to treatment.

Table III-4. DCP Requests for CPMRS Information (2008-2015)			
Researcher (DATE)	**General Purpose**	**Outcome**	**MOU Requirements**
Purdue (2010)	Part of a series of epidemiology studies to measure risk and impact of a particular drug formulation	Request approved - Provided de-identified data per MOU	• Confidentiality provision specific to personal health information • Preview of publication
Brown (2010-12)	Part of a CDC research grant on unintentional poisoning deaths	Request approved - Provided de-identified data per MOU	• HIPAA compliance • Confidentiality provision for use and disclosure of data including PHI • Discussion of data safeguards • Report and handling of improper data use or disclosure • Return/destruction of PHI and dataset • Review of final results
DMHAS (2011)	Study on non-medical use of narcotic prescriptions	Request approved - Provided de-identified data per MOU	• Description of roles/responsibilities for data linking process to protect personal identifying data • Return/destruction of files in DCP presence • Specific mention of state/federal privacy laws • Review of final results
Brown (2013)	To improve pharmacy practice, safer opioid prescribing, and patient care	Request denied - Required identifiable information	N/A
University of Pennsylvania (2014)	To compare prescribing behaviors to improve clinical decision-making software	Request denied - No IRB from the university; determined to be marketing scheme	N/A
CT Poison Control & Medical Examiner (2015)	To work on a joint study (details unavailable)	Request pending	N/A
Source: PRI staff analysis			

University requests. There were two university requests approved by DCP - Purdue and Brown. The MOU with Purdue clearly stated the research objective, contained general confidentiality provisions pursuant to state law, and granted pre-publication comment. Although the information provided was de-identified, there was no mention of data retention or disposal methods. The confidentiality language reads as follows:

> Purdue and CPMP agree that the disclosure of Protected Health Information (PHI) or Personal Information (individually identifiable health information, employment information, insurance information or family information) is not required under this Agreement. If performance under this Agreement involves the inadvertent disclosure of PHI or Personal Information, the receiving party shall notify the other party promptly upon discovery. The receiving party agrees to make available in a reasonable time and manner any information needed by the other party, PHI or Personal Information will be transmitted, handled, stored, maintained, used, and destroyed in a manner that will preserve its confidentiality and is consistent with all applicable laws.[55]

The MOU with Brown University provided detailed provisions regarding the researcher's roles and responsibilities; compliance with HIPAA requirements; use and disclosure of personal health data; location safeguards; immediate report of improper use, disclosure, or breach; and return/destruction of data at conclusion of project.

De-identification. In the few instances where an information request was granted, DCP did not have its own de-identification policy or process. It followed the DMHAS protocol for de-identification. This consisted of having the researcher extract data fields from the database in the presence of DCP staff to ensure personal identifiable information was not taken. Since that time, Optimum, the database vendor, has created a database function that allows the PMP program administrator to produce reports and queries without identifiable data fields.

Review process. A review of the requests for CPMRS information from public and private entities indicates there are no formal written DCP policies and procedures in place to handle these inquiries. As mentioned earlier, requests are considered on a case-by-case basis. Unlike the data request process at DPH, DCP does not have formal criteria, guidelines, or process steps to determine disclosure of information to public or private entities. DCP does not receive many requests (six requests in seven years) so a formalized process is rarely needed. However, best practice suggests a formal written process outlining submission requirements, criteria, and guidelines used to review requests. Best practice also involves standard terms and conditions for use agreements including penalties for data misuse or disclosure violations.

Vendor contract. As noted previously, Optimum is the contracted vendor serving as the CPMRS system administrator since the program's launch in 2008. The contract was renewed in 2013 and is set to expire January 22, 2016. In addition to the statutory requirement prohibiting information disclosure and mandating compliance with confidentiality laws, the contract between DCP and the vendor contains specific confidentiality and nondisclosure provisions:

[55] *Connecticut Prescription Monitoring Program Project Agreement 120610*, Section 5, p.2 (December 2010).

> All material and information provided to the Contractor by the State or acquired by the Contractor in performance of the Contract whether verbal, written, recorded magnetic media, cards or otherwise shall be regarded as confidential information and all necessary steps shall be taken by the Contractor to safeguard the confidentiality of such material or information in conformance with federal and state statutes and regulations. The Contractor agrees that it is prohibited from releasing any and all information provided by the Department or providers or any information generated by the Contractor without the prior express written consent of the Department.[56]

The contract also stipulates that all department information exposed or made available to the contractor is to be considered and handled as confidential and is not to be removed, altered or disclosed to others in whole or in part by the contractor. These confidentiality provisions survive the termination of the agreement.

Compliance. Based on interviews with PMP staff, there does not seem to be any check or verification of compliance with some written agreement provisions. For example, the Optimum vendor contract for CPMRS operation and maintenance was executed in 2008 and security safeguards pursuant to the contract were verified by an outside third-party user (i.e., PMP program management in an adjoining state to the vendor). According to Connecticut PMP management staff, the vendor and contract requirements were vetted by the federal Department of Health and Human Services (HHS). The PMP program management staff also noted that BEST had reviewed the vendor contract. Similarly, researcher compliance with MOU provisions are not checked or verified. The PRI committee staff acknowledges that it may not be feasible for the department to dispatch limited DCP staff resources to verify compliance with written agreements.

National Association of Boards of Pharmacy (NABP). DCP entered into a MOU with the National Association of Boards of Pharmacy (NABP), a non-profit professional organization, in 2011. Through the MOU, the board acts as an interstate data-sharing hub server providing states with a PMP interconnect system that allows participating states access to out-of-state PMP information. There is no cost for the state interconnection service. The MOU expires on June 30, 2016.

The MOU stipulates that the NABP must develop and maintain the hub system in accordance with state requirements, industry standards, and laws and rules applicable to protected health information and personally identifiable information. The NABP cannot access or use any protected health information and/or personally identifiable patient information that is transmitted through the hub system. System users must meet the individual criteria designated by each state to access that state's PMP information. Each participating state agrees to investigate another state's complaint against a state-authorized user for failure to comply with applicable state or federal laws or rules, other state requirements for access or use of PMP information, or system requirements.

[56] *State of Connecticut, Department of Information Technology Master Agreement #06ITZ0108MA*, Section 14, p.13 (January 2008).

Other states. Currently, 30 states are enabled to securely share PMP data through the NABP interconnect server. However, as noted above, states must have similar access requirements in order to share information.[57] As a result, Connecticut's interstate data-sharing includes 17 other states, only one of which is in New England or a bordering state (Arizona, Colorado, Delaware, Illinois, Indiana, Kansas, Michigan, Minnesota, New Jersey, New Mexico, Nevada, North Dakota, Ohio, Rhode Island, South Dakota, Utah, and Virginia.)

The MOU with the NABP cancels the need for individual MOUs among the states, unless the state also requires it. For this reason, the Connecticut PMP has also entered into a MOU with the state of New Jersey. The purpose of the MOU is to establish the terms of participation by which each PMP program agrees to disclose prescription monitoring information to authorized users in its respective program. The MOU includes terms guiding the information to be disclosed, the use of the information, privacy and security safeguards, authorization of users, retention of information, and confidentiality.

Only PMP information normally provided upon request to an authorized practitioner or pharmacist may be disclosed to authorized practitioners or pharmacists in the requesting state. The PMP information can only be used for mandated program purposes and cannot be released or disclosed to any other person or entity. Each state must require authorized users (i.e., a practitioner or pharmacist) to certify at the time a request is made that they will adhere to the requesting state's applicable laws and restrictions on the use and disclosure of the PMP information.

All web services used between the participating states and the hub server must employ industry standard data encryption methodology. Furthermore, all protected health information must be encrypted using advanced encryption methodology. This dual encryption design must meet the most current version of Federal Information Processing Standards (FIPS) and is intended to provide secure data transmission.[58]

The MOU between Connecticut and New Jersey specifically addresses confidentiality with a provision stating:

> Unless otherwise required by law, each party shall keep confidential all information, in whatever form, produced, prepared, observed, or received by that party to the extent that such information is confidential by law or otherwise required by this MOU; except that the information may be provided to the authorized requestor (end user) of the prescription monitoring program for the purposes allowable, and with the documented restrictions that are provided under each state's applicable statutes and regulations.[59]

[57] For example, if a state allows users to share accounts or have delegates (e.g., doctor and nurse), then only states with similar policies can share data.
[58] FIPS are publicly announced standards developed by the U.S. federal government for use in computer systems by non-military government agencies and government contractors. FIPS standards are issued to establish requirements for various purposes such as ensuring computer security and interoperability.
[59] *Memorandum of Understanding Between the State of New Jersey and the State of Connecticut*, Section 9, p.6, (June 2013).

Requested PMP information may be viewed as a report image but cannot be stored in the requesting state's database and is subject to the system's audit trail. Any discovery of a security incident involving successful unauthorized access, use, disclosure, modification, or destruction of PMP information must be reported within 10 days.

Notice and disclosure to individuals. Statutory mandates regarding the disclosure of information maintained by state agencies are found in both the state Personal Data Act (PDA) and the individual agency statutes corresponding to the specific programs related to the databases.

Personal Data Act (PDA). There are two specific PDA provisions relating to the disclosure of information maintained by state agencies. According to the PDA, state agencies must:

- disclose to a person, upon written request, all personal data concerning him or her that is maintained by the agency, as well as any record of authorized disclosures of information; and
- keep a record of any individual, agency, or organization that obtains access to personal data and the reason for this access.[60]

Additionally, the PDA gives an individual the right to contest the accuracy, completeness, or relevancy of their personal data.[61] If the agency disputes any changes requested by an individual, the person has the right to submit a letter outlining his or her concerns and corrections, which then becomes a permanent part of the agency's personal data system.

The PRI committee staff asked DPH and DCP about the applicability of these PDA requirements to the specific programs under PRI review. According to both agencies, information maintained by the individual state programs is exempt from PDA disclosure. Each agency cited the statutory confidentiality mandates for the individual program as dictating access to information. Currently, neither program's statutory authority permits disclosure to the public or to the individual who is the subject of the data.

It should be noted that eleven other states with prescription monitoring programs (CO, KS, MD, MN, OR, PA, RI, UT, VA, VT, WV) and D.C. require prescribers, dispensers, or other entities to post or distribute written notice to consumers that their prescription information is being submitted to the PMP and may be accessed by certain persons or entities.[62] In addition, 39 states and D.C. allow patients or an individual on behalf of a patient to receive their dispensing data from the PMP.[63]

[60] C.G.S. Sec.4-193.
[61] C.G.S. Sec.4-193(h).
[62] National Alliance for Model State Drug Laws (NAMSDL), *Annual Review of Prescription Monitoring Programs* (2015) p.9., Research current through September 2015.
[63] National Alliance for Model State Drug Laws (NAMSDL), *Annual Review of Prescription Monitoring Programs* (2015) p.26., Research current through September 2015.

Separate discussions between the PRI committee staff and DCP program management staff as well as members of organizations representing prescribers and dispensers suggest some drawbacks to requiring notice and disclosure to consumers. Currently, requests for PMP information are managed by the program administrator, essentially the sole staff person for PMP. It is unclear what impact allowing requests for information to consumers would have on the program's workload without additional staff resources. Another concern is whether consumer notice of monitoring would in some way produce a chilling effect on individuals seeking medical care. Without further examination of the policy impact, the PRI committee staff makes no recommendation in this area.

Key Staff Findings: DCP Information Sharing

- Audits of active case numbers used by registered CPMRS law enforcement officials are rarely done.
- Unlike the data request process at DPH, DCP does not have formal criteria, guidelines, or procedural steps to determine whether to disclose CPMRS information to public or private entities for research purposes.
- The executed written agreements guiding the disclosure of CPMRS information for research purposes contain provisions for the use and confidentiality of personal health information.
- There is no standardized agency language for written agreements regarding confidentiality provisions for the access to CPMRS information.
- Similar to DPH, DCP does not verify compliance of provisions within written agreements.

Staff Recommendations: DCP Information Sharing

16. **DCP should periodically conduct random audits of law enforcement use of active case numbers in the CPMRS system.**
17. **DCP should establish and implement written policies and procedures for the submission and approval of CPMRS information requests from public or private entities for research purposes.**
18. **DCP should develop standard language for written CPMRS/PMP information sharing agreements that address specific state confidentiality statutes, penalties for violations of any disclosure or misuse of information, and requestor responsibilities for data retention and destruction.**
19. **Within available resources, DCP should attempt to verify authorized CPMRS information receivers' compliance with administrative, physical, and technical safeguard terms and conditions outlined in written CPMRS/PMP agreements.**

APPENDICES

Appendix A

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 Disease 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 Disease 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
Michelle Castillo: Michelle.Castillo@cga.ct.gov
Alexis Warth: Alexis.Warth@cga.ct.gov

Appendix B

PRI Data Collection Tool

All 65 questions of the PRI data collection tool are listed below. The number and types of questions asked of each interviewee were adjusted based on the topic and context of the interview.

Administrative Safeguards
Policies and Procedures
1. Are there up-to-date policies, published and communicated to employees regarding:
a. Confidentiality? - If yes, please provide a copy
i. If yes, is the policy department wide or section specific?
ii. Is the policy comprehensive and enforceable?
iii. When was the policy last updated?
iv. Who (what departments/agencies) was involved in the policy development?
b. Technology/equipment usage? - If yes, please provide a copy
i. If yes, is the policy department wide or section specific?
ii. Is the policy comprehensive and enforceable?
iii. When was the policy last updated?
iv. Who (what departments/agencies) was involved in the policy development?
c. Data handling? - If yes, please provide a copy
i. If yes, is the policy department wide or section specific?
ii. Is the policy comprehensive and enforceable?
iii. When was the policy last updated?
iv. Who (what departments/agencies) was involved in the policy development?
d. Are there any other department/section policies that address data security?
2. Does the department/section have a risk management plan? - If yes, please provide a copy
a. If yes, is the plan department wide or section specific?
b. Does the plan include:
i. A data back-up plan?
ii. A disaster recovery plan?
iii. An emergency mode operation plan?
c. Has the plan been implemented?
d. How often does the section conduct risk assessments?
3. Are employees provided with explanation and/or training of the policies in Question 1?
a. Are employees required to sign each of the policies in Question 1?
b. If yes, when do they sign?
c. Are staff ever required to re-sign the policies?

Administrative Safeguards
Policies and Procedures
4. Are there written consequences for violating any of these policies?

5. Who is responsible for ensuring that the following policies are followed? (name and title)
a. Confidentiality?
b. Technology/equipment usage?
c. Data handling?
d. How is this oversight conducted?
e. How many violations have been documented in the past three years?
f. What have been the consequences of these violations?

6. Does the department/section keep an up-to-date asset inventory?
a. Are physical devices/systems inventoried?
b. Are software and applications inventoried?
c. Are external information systems inventoried?

Appropriateness of Information Collected
7. Who determines what data fields are collected for the database? (name and title)
a. How is it decided what information is "minimally necessary"?
b. Is there compliance with statutorily required data fields?
c. How often are these fields changed/evaluated?
d. Have we been provided with the current data definitions?

8. Does the department/section have up-to-date data classifications for these fields?

Information Sharing
9. Is there a written policy describing the information sharing process, procedures, and criteria?
a. For registered users? For requests from third parties (such as researchers)?
b. Does this policy comply with statutory and regulatory requirements?

10. Is there a formal review process for information requests from third parties?
a. Are the results of this process recorded/documented?
b. In the past three years, how many requests have been received? Approved? Denied?

11. Does the department/section have a written policy concerning data de-identification?
a. Does this policy comply with statutory and regulatory requirements?

Administrative Safeguards
Information Sharing
12. Is there privacy and security language included in data sharing agreements with:
a. Other state agencies?
b. Federal government agencies?
c. Local government agencies?
d. Contractors/vendors?
e. Registered users?
e. Other third parties (such as researchers) ?
f. Who approved the contract language for legal and statutory compliance? (name and title)
g. What is the oversight process to ensure compliance with contract security requirements?
h. Are there written consequences for violations of the contract security requirements?

Physical Safeguards
Building Security
13. Are there formal, written policies and procedures that limit unauthorized physical access to personal health information?

14. Is each department employee provided with a photo ID badge?
a. Are employees required to show their badge prior to entering the building?
b. Are there audit records of who has accessed the secure areas of the building?
c. How often are the audit records reviewed?

15. Does the section share a building with other departments?
a. If yes, is the section physically separated from other departments?
b. Are all visitors required to sign-in when entering the building?
c. Are all visitors required to be escorted by an employee?
d. How are project files and electronic equipment physically secured?

16. Do individuals who are not project staff have access to work areas?

17. Is there a policy outlining requirements for securing physical copies of information when a staff person is away from their desk?
a. If yes, which policy?
b. Does this policy include procedures during an emergency?

Mail Handling/Security
18. Is there a written policy/procedure for mail handling and security regarding personal health info?

19. Is there a secure/limited access area where incoming and outgoing mail is placed?

Physical Safeguards
Mail Handling/Security
20. Who is responsible for (1) receiving, (2) sorting, and (3) distributing mail? (name and title)
a. How is the mail distributed to the project?

Fax Handling/Security
21. Is there a written policy/procedure for fax handling and security regarding personal health info?

22. Does the project have its own dedicated fax machine?
a. Do any individuals who are not project staff have access to the fax machine?
b. Is the fax machine located in the project's work area?

23. Is there a requirement for the timely retrieval of incoming faxes?

24. Is there a standard disclaimer included on all incoming and outgoing faxes?

Phone Handling/Security
25. Is there a written policy/procedure for phone usage regarding personal health info?
a. Is personal health information gathered over the phone documented?
b. If yes, how is this documentation handled/protected?

Printing Handling/Security
26. Is there a written policy/procedure for printer usage regarding personal health info?

27. Does the project have a dedicated printer?
a. Is the printer located in the project's work area?

28. Is the printer secured using either project-specific or staff-specific release codes?

Email Handling/Security
29. Is there a written policy/procedure concerning the inclusion of personal health information in emails?
a. Are incoming and outgoing email transmissions encrypted?
b. What steps are taken if inappropriate personal health information is found in an email?

Paper Record Handling
30. Does the department have a record retention policy for written records? For electronic records?
a. How long does the project keep records?

31. While being used, are paper records stored in locked drawers/cabinets?

Physical Safeguards
Paper Record Handling
32. Once records are no longer active, are they moved to long-term storage?
a. When are records are considered "inactive"?
b. Is long-term storage on-site or off-site?
c. During long-term storage, are records kept in locked cabinets?
d. Are the cabinets in a locked room? Who has access?

33. Who is responsible for overseeing proper record handling and retention? (name and title)

34. Are storage and disposal services contracted?
a. Is there contract language regarding the proper handling of confidential information?
b. How does the project confirm that records are disposed of properly?

Technical Safeguards
Computer Access and Usage
35. Do non-project staff have physical access to project computers?

36. Are staff provided with individual workstation log-in credentials?
a. How often are staff required to change their password?

37. Do all computers use a password protected screensaver function?

38. Do any of the policies contain language requiring staff to lock their computers prior to leaving their desk?
a. If yes, which policy?

39. Are staff able to save files on their computer hard drive or an external storage devices?

40. Do all computers have anti-virus software installed?
a. How often is the software updated?

41. Are records kept of staff log-in activity?
a. If yes, how often are records reviewed for indications of inappropriate or unusual activity?

42. Does the section utilize encryption for their internet access?
a. If yes, what encryption standard is used?

Technical Safeguards
Computer Access and Usage
43. Do any of the department/section policies address the storage or access of personal health information on portable devices and/or personally owned devices?
a. If yes, which policy?

File Server Security
44. Does the project store any personal health information on the file server?

45. Is there a formal, documented, access control policy that addresses:
a. What projects, sections, and/or departments use the file server
b. Type of data stored on the file server
c. Roles and responsibilities for server usage
d. Security measures to protect server data
e. Audit and accountability tools, policies, and procedures

46. Are file server drives/folders password protected?
a. If yes, who determines each staff person's access level? (name and title)
b. Is access to shared drives/folders position, project, or section specific?
c. How many people have access to the project's file server(s)?
d. Is server access recorded?
i. How often are records reviewed for indications of inappropriate or unusual activity?

47. Are file servers protected by a firewall?
a. Who administers and monitors the firewall? (department/agency)

48. How often is security software updated?

49. Are the physical file servers kept in a secured area?
a. Are servers stored on-site or off-site?
b. How many people have access to this secured area?
c. How is access determined?
d. Are there audit records of who has access the secure area?

50. How often are file servers backed up?
a. Are these back-ups encrypted?
b. What encryption standard is used?

Technical Safeguards
Database Management and Security - Technical Framework and Infrastructure
51. Who initially created the database? (department, title, name)

52. Who currently oversees the technical maintenance of the database? (name and title)
a. Where are the database servers currently located?
b. Are the database servers in a secure area? Who has access?

53. Is there a formal, documented access control policy that addresses:
a. Database purpose
b. Scope of data collected/stored
c. Roles and responsibilities of database usage
d. Compliance requirements for stated policies and procedures
e. Audit and accountability tools, policies, and procedures

54. What security standards are currently utilized in the database? (firewalls, encryption, etc.)

55. Does the database generate audit records for (1) user access, (2) record creation/editing, and (3) any downloads of data?
a. Is location of activity recorded? (internal vs. remote)
b. Is date of activity recorded?
c. Is time of activity recorded?
d. How long are audit records retained?

56. What is the current protocol for removing inactive users (former employees, contractors, etc.)?
a. Do users get locked out after a certain period of inactivity? (no sign-in for weeks/months)?

57. Does the database automatically lock a user out after a certain number of unsuccessful log-in attempts?

58. Does the database allow for concurrent sign-ins with a single username?

59. Does the database automatically log a user out after a certain number of inactive minutes?

60. What protections and processes have been implemented to identify the occurrence of and response to a cybersecurity event? (continuous security monitoring, detection process, etc.)
a. How many data breaches have been documented by this project? What was the outcome?

61. How often is the database server backed up?
a. Is the back-up on-site or off-site?

Technical Safeguards
Database Management and Security - Technical Framework and Infrastructure
b. Is the back-up encrypted? What encryption standard is used?

Database Management and Security - Management and Oversight
62. What permission levels exist in the database?
a. Who is responsible for assigning permission levels? (name and title)
b. Does the administrator use the concept of "least privilege" when assigning permissions?
c. Is there any oversight or auditing mechanism to confirm appropriate assignment of permissions?
d. How many users are currently assigned to each permission level?

63. Is each user given a unique username and password?
a. How often are staff required to change their password?
b. Is there a protocol for auditing for sign-in sharing?
c. Who is responsible for establishing new user accounts? (name and title)
c. Does the project maintain an inventory of current users?
d. How many user accounts exist today?

64. How often does the project review/analyze audit records for indications of inappropriate or unusual activity?
a. Is there a documented procedure for addressing concerns?
b. How many formal concerns have been raised over database activity in the past three years?

65. When a user signs into the database, is a notification displayed outlining (1) appropriate use, (2) that actions are monitored, and (3) consequences for abuse of the system?

Appendix C

PRI Data Collection Tool Source Descriptions

Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Prior to the passage of HIPAA in 1996, no generally accepted set of information security standards or requirements existed in the health care industry.[1] While neither of the programs discussed in this report are considered *covered entities* under HIPAA, the guidelines and safeguards within the law are considered best practices for any entity handling sensitive health information. The Security Rule within HIPAA outlines a set of required and recommended safeguards that, when combined, limit the risk of security or confidentiality breaches within an entity.

National Institute of Standards and Technology (NIST). Following the issuance of federal Executive Order 13636 in 2013, the National Institute of Standards and Technology was charged with the creation of a "set of industry standards and best practices to help organizations manage cybersecurity risks."[2] In 2014, NIST published a *Framework for Improving Critical Infrastructure Cybersecurity*. This framework was created through collaboration between government and the private sector, and sought to "address and manage cybersecurity risk in a cost-effective way."[3] The NIST framework has become a best practice within the information security field, and is currently used as reference by multiple agencies within Connecticut, including the State Auditors of Public Accounts and the Department of Administrative Services' Bureau of Enterprise Systems and Technology (BEST).

Center for Disease Control and Prevention (CDC). The Center for Disease Control and Prevention regularly publishes *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs* for use by public health authorities across the country.[4] The legal privacy and security requirements for HIV/AIDS related information are considered some of the most stringent within the medical field. The *Data Security* document includes specific security guidelines for the collection, use, storage, and sharing of protected health information that meet the strict requirements for the handling of HIV related data.

International Organization for Standardization (ISO). The International Organization for Standardization (ISO) developed a group of standards that focus specifically on "helping organizations keep information assets secure."[5] This section of standards outlines requirements for an information security management system (ISMS), which ISO defines as a

[1] Department of Health and Human Services. March 2007. Security Standards: Security 101 for Covered Entities. *HIPAA Security Series*, Volume 2 (Paper 1), p.3.
[2] National Institute of Standards and Technology. February 2014. *Framework for Improving Critical Infrastructure Cybersecurity.*
[3] Ibid.
[4] National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention. 2011. *Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs*. Center for Disease Control.
[5] ISO 27001 – Information security management.

systematic approach, including people, processes, and IT systems, to manage sensitive information.

State statutes and regulations. In addition to the data protection requirements in the Connecticut Personal Data Act, information handling within both DCP and DPH is dictated by department specific state statutes and regulations. In addition to department specific laws, both DCP and DPH are subject to statutes, regulations, and policies distributed by other state agencies, including the Office of Policy and Management (OPM), Department of Administrative Services (DAS), and Bureau of Enterprise Systems and Technologies (BEST). Statutes and regulations provide requirements in areas such as information confidentiality, data classification, staff training, data protection, and authorized information sharing. Specific requirements found within statutes and regulations were integrated into the PRI data collection tool to measure each department's compliance with state legal requirements.[6]

[6] See Appendix D for specific statutes and regulations for DPH and DCP.

Appendix D

Relevant State Statutes and Regulations

General Responsibilities
Applicable to both IDS and PMP

Personal Data Act (C.G.S. Sec. 4-193) – Agencies are responsible for:

- Informing all employees of the Personal Data Act, department regulations, and Freedom of Information Act
- Protecting data from fire, theft, flood, natural disaster, and other physical threats
- Recording every individual, agency, or organization who obtains access to personal data
- Collecting and maintaining only that information about a person which is relevant and necessary to accomplish the agency's lawful purposes
- Releasing data when requested and only when such release is legally permissible
- Creating procedures for accessing and releasing data

C.G.S. Sec. 1-84a – Prohibits the disclosure of confidential information for financial gain obtained in the course of official duties after leaving state employment

DPH IDS	DCP PMP
Conn. Agency Regs. Sec. 19a-2a-23 – Only department staff who have specific need to access information shall have access *C.G.S. Sec. 19a-25* – All personal health information collected by IDS is confidential and can be used solely for the purposes of medical scientific research, and for disease prevention and control	*C.G.S. Sec. 21a-254(j)* – Authorizes DCP to establish an electronic prescription drug monitoring program to collect prescription information on controlled substances *Conn. Agency Regs. Sec. 21a-1-7a* – All employees who function as custodians of personal data systems or who have access shall: ○ Be given a copy of the provisions of Chapter 3 (Public Records) and 55 (Personal Data Act) of C.G.S., as well as a copy of DCP regulations ○ Take reasonable precautions to protect personal data from fire, theft, flood, natural disaster, and other physical threats ○ Maintain a record of each person, individual, agency or organization who has obtained access to or to whom disclosure has been made of personal data

Data Collection	
Applicable to both IDS and PMP	
OPM Data Classification Policy – Each Executive Branch Agency shall assign a classification to all data for which the agency has custodial responsibility, following the Data Classification Methodology as developed and provided by DOIT	
DPH IDS	**DCP PMP**
Conn. Agency Regs. Sec. 19a-2a-12 and *19a-36-A4*– IDS data fields include, but are not limited to: name, address, age, date of birth, race, sex, occupation, attending physician, and any behaviors that may have increased chance of exposure *Conn. Agency Regs. Sec. 19a-2a-23* – Personal data shall not be maintained if not relevant and necessary for the lawful purpose of the agency	*C.G.S. Sec. 21a-254* – PMP required data fields include: Dispenser ID number Date prescription was filled Prescription number Patient ID number Patient first and last name Patient address Patient date of birth Prescribing physician's DEA number Type of payment
Information Sharing	
DPH IDS	**DCP PMP**
Conn. Agency Regs. Sec. 19a-2a-23(f) – The department shall incorporate provisions of the Personal Data Act in all contract, agreements, or licenses *Conn. Agency Regs. Sec. 19a-7-2* – • Aggregate health data shall not include personal data or patient-identifiable data[7] • Any release of aggregate data is only for public health purposes *Conn. Agency Regs. Sec. 19a-25-3* – Identifiable health data can only be released to: ○ Health care providers in a medical emergency ○ Health care providers, local health directors, another state or public health agency, or other persons deemed necessary, for disease prevention and control	*Conn. Agency Regs. Sec. 21a-1-7a* - Department is not required to release information to an individual if precluded by law *Conn. Agency Regs. Sec. 21a-254-4* – DCP may provide prescription information to: • Other regulatory, investigative, or law enforcement agencies for disciplinary, civil, or criminal purposes • Practitioners, for the purpose of education • Practitioners, for patient care • Pharmacists, for patient care • Public or private entities, for statistical, research, or educational purposes, provided that patient privacy and confidentiality of patient information are not compromised

[7] DPH references the de-identification standard outlined in 45 C.F.R. 164.514.

Information Sharing (cont'd)	
DPH IDS	**DCP PMP**
○ Individuals, organizations, government entities, and/or federal entities for medical or scientific research ○ Government entities for purpose of conducting an audit, evaluation, or investigation required by law of the department • The department shall release only the minimum amount of data necessary • Requests for medical or scientific research shall be submitted through a written application ○ Approved requests require a written agreement confirming the use, protection, and destruction of provided data • No identifiable health data obtained by IDS shall be subject to subpoena	
Physical Security	
DPH IDS	**DCP PMP**
Conn. Agency Regs. Sec. 19a-2a-12 – Records are retained in accordance with Connecticut State Library record retention policies *Conn. Agency Regs. Sec. 19a-2a-23* – • Only department staff who have specific need to access information shall have access • Department electronic data systems shall: ○ Locate equipment and records in a limited access area ○ Require visitors to areas to sign a visitor's log, on a need-to-enter basis only ○ Limit regular access to operations personnel ○ Utilize appropriate access control measures to prevent unauthorized disclosure of personal data • All manual records are kept under lock and key, and to the greatest extent practical, in controlled access areas	*C.G.S. Sec. 21a-254* – Records are kept for a period of three years from the date the transaction is recorded *Conn. Agency Regs. Sec. 21a-326-3* – DCP shall maintain records in accordance with applicable state and federal laws, rules, and regulations

Technical Safeguards	
Applicable to both IDS and PMP	
BEST Mobile Computing Policy *BEST Acceptable Usage Policy*	
DPH IDS	**DCP PMP**

Conn. Agency Regs. Sec. 19a-2a-12 –
• Regulations outlining the purpose, authorized users, data fields, and management of IDS databases
• IDS is authorized to receive data from:
  o Health care providers
  o Health care facilities
  o Medical laboratories
  o Department of Correction
  o Schools
  o Local directors of health
• Only department staff and authorized researchers have access to IDS database
 	
Conn. Agency Regs. Sec. 19a-2a-23 –
• Only department staff who have specific need to access information shall have access
• Department shall maintain a written, up-to-date list of individuals entitled to access each personal data system
• Department electronic data systems shall:
  o Locate equipment and records in a limited access area
  o Require visitors to areas to sign a visitor's log, on a need-to-enter basis only
  o Limit regular access to operations personnel
  o Utilize appropriate access control measures to prevent unauthorized disclosure of personal data
	C.G.S. Sec. 21a-254 –
	• DCP Commissioner may contract with a vendor for electronic collection of prescription information
	• Electronic PMP database may be accessed by prescribing practitioners, for the purpose of treating a patient, and pharmacists who are dispensing a controlled substance
	
	Conn. Agency Regs. Sec. 21a-254-4 –
	• Pharmacies transmitting information electronically to PMP must submit the information included in the most recent edition of the Electronic Reporting Standard for Prescription Monitoring Programs
	• Information shall be transmitted through
	  o A computer modem that can transmit information at a rate of 2400 baud or more
	  o Computer disc
	  o Magnetic tape
	
	Conn. Agency Regs. Sec. 21a-326-3 – It is the responsibility of the registrant who ceases to practice or who goes out of business to notify the DCP Commissioner in writing 5 days before such occurrence