

Legislative Program Review and Investigations Committee

Senate Members

John W. Fonfara, *Co-Chair*
John A. Kissel
Eric D. Coleman
Anthony Guglielmo
Joe Markley
Andrew Maynard

Connecticut General Assembly

State Capitol Room 506
Hartford, CT 06106
Phone (860) 240-0300
Facsimile (860) 240-0327
www.cga.ct.gov/pri/index.asp

House Members

Christie M. Carpino, *Co-Chair*
Mary M. Mushinsky
Whit Betts
Henry Genga
Philip Miller
Cara Pavalock

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 15-182 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