



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 health 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.

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.