REPORT OF THE SECRETARY OF HEALTH AND HUMAN RESOURCES

Report on Implementation of HB2457 – Data Sharing Among State Health and Human Resource Agencies (Chapter 467, 2017)

**TO THE GOVERNOR AND
THE GENERAL ASSEMBLY OF VIRGINIA**

HOUSE DOCUMENT NO. 3

**COMMONWEALTH OF VIRGINIA
RICHMOND
2018**

COMMONWEALTH of VIRGINIA

Office of the Governor

William A. Hazel, Jr., MD
Secretary of Health and Human Resources

January 10, 2018

Members, Virginia General Assembly
900 E. Main Street
Richmond, Virginia 23219

RE: Report on Implementation of HB2457 (Data sharing within the Secretariat of Health and Human Resources).

Dear Legislators:

I am pleased to submit this report on implementation of House Bill 2457 (2017) which adds language to §2.2-212 of the Code of Virginia authorizing state Health and Human Resource agencies to share data. If you have questions or need additional information concerning the report, please contact my office.

Sincerely,

William A. Hazel, Jr., M.D.

Attachment

REPORT ON IMPLEMENTATION OF HB2457

DATA SHARING AMONG STATE HEALTH AND HUMAN RESOURCE AGENCIES

House Bill 2457 passed during the 2017 session of the Virginia General Assembly and amended section § 2.2-212 of the Code of Virginia. The Bill added to this section of the Code paragraph (B) which states:

"As requested by the Secretary of Health and Human Resources, and to the extent authorized by federal law, the agencies of the Secretariat of Health and Human Resources shall share data, records, and information about applicants for and recipients of services from the agencies of the Secretariat, including individually identifiable health information for the purposes of (i) streamlining administrative processes and reducing administrative burdens on the agencies, (ii) reducing paperwork and administrative burdens on applicants and recipients, and (iii) improving access to and quality of services provided by the agencies. The bill requires the Secretary of Health and Human Resources to report on the implementation of the provisions of the bill by October 1, 2017."

The following is a summary of agency activities in response to the bill, followed by a section with recommendations for additional actions that could be taken to further the goals described in the bill.

Agency Data Sharing Activities

Most agencies within the Health and Human Resources Secretariat (HHR) have no formal policy or process for responding to requests for data from outside the agency. Since HB2457 was signed into law several HHR agencies have begun reviewing their data sharing policies, procedures, and existing agreements. Some have developed or enhanced existing forms and templates for data sharing and non-disclosure agreements.

In addition, the Department of Social Services, Department of Aging and Rehabilitative Services, Department of Health Professions, and most recently the Office of Children's Services participate in the Virginia Longitudinal Data System (VLDS) which is a data sharing platform enabling client-level information to be linked across participating agency data sets and shared in de-identified form for research purposes.

The Department of Social Services (DSS) has developed formal guidance and a process for handling external data requests. Efforts are focused on developing a standard request form and a template for data sharing agreements to incorporate more explicit instructions and requirements for data handling and security, as well as limitations on use of the data.

The Department receives many data requests each year from state agencies, cities and local departments of social services, researchers conducting work under contract with federal, state, and

local government offices, and from independent researchers (universities). In every case, approval to share the data must be based on who is asking, what data they are requesting, and what the purpose is for which they will use the data? Each request must be evaluated to determine whether it meets one or more of the allowed exceptions governing the sharing of the data in question.

DSS is also working to create an automated workflow solution that will store information about each request and route them to appropriate personnel for review and approval, based on details provided by the requestor.

The Office of Children's Services (OCS) does not have formal guidance or process for data sharing. It receives relatively few requests for data each year and handles them on a case by case basis. Recently, OCS has completed a project to prepare a data set that can be shared using the VLDS. The data represent services received by foster care and at-risk youth.

The Department of Aging and Rehabilitative Services (DARS) receives very few data requests each year and does not have formal data sharing guidance or process. It reviews each request for compliance with legal authority and security standards and requires a contract or MOU specific to the purpose of the data exchange. DARS also participates in the Governor's Data Internship Program (GDIP) which utilizes data sharing with interns on short-term projects focused on policy and service issues.

The Department of Health (VDH) has a data governance group that is currently working to implement a more formal process for data sharing, including the development of a standard template for data sharing agreements that will be required anytime data with personally identifiable data, or other sensitive data are shared with external parties, including other state agencies. VDH does not plan to centralize the data-sharing process across the agency, opting instead to provide guidance and expectations to data stewards at the state and local levels.

New data sharing activities at VDH include a collaborative effort with the Department of Behavioral Health and Development Services (DBHDS) in which the agencies completed the first phase in an effort to match DBHDS's data against VDH's death records with the goal of enhancing DBHDS's data accuracy. More recently, VDH and the Department of Medical Assistance Services (DMAS) are in the early stages of planning a bi-directional data sharing effort regarding Neonatal Abstinence Syndrome (NAS) data.

Two years ago the DMAS implemented an agency-wide data governance program. A committee led by the Policy Division has been formed to explore modifications to DMAS' data sharing policies with the goal of streamlining the data request process, FOIAs, and sharing in accordance with HIPAA (Health Insurance Portability and Protection Act). The agency is developing an automated data sharing work flow to facilitate the process of reviews and approvals when requests come in.

The Department of Health Professions' (DHP) does not have formal guidance or process for data sharing requests. It has an online License Lookup tool that provides open access to data on over 370,000 health practitioners and facilities, including links to disciplinary public records. Additionally, the Department's Healthcare Workforce Data Center (HWDC) maintains licensee workforce survey data and the Prescription Monitoring Program (PMP) Schedule II-IV prescription drug data to assist in deterring the

illegitimate use of prescription drugs. The agency makes other data available through the VLDS and project-specific data sharing agreements. DHP shares survey data with VDH to streamline and enhance the Commonwealth's federal Health Professional Shortage Area and Medically Underserved Area designation efforts. PMP data is also shared through other agreements, most recently with VDH to provide de-identified data sets for health oversight activities and to provide performance measure data related to a Centers for Disease Control Prevention for States Grant.

Recommendations

1 - HB2457 states that as requested by the Secretary of HHR and as permitted by federal law, HHR agencies shall share data. It is not clear whether this means HB2457 supersedes other state law regulating the sharing of data collected and maintained by HHR agencies. It would be helpful if a legal opinion from the Office of the Attorney General were provided to HHR agencies on this question.

2 - While several agencies within HHR are working to develop and implement more formal, streamlined approaches to data sharing within their agency, there is a need for standardization and coordination across agencies as well. There is also a need for guidance to help agencies understand what types of data sharing are permissible (or not permissible), and a mechanism to make data sharing simple and secure.

For example, consent is an important element of data sharing. Proper opt-in and opt-out mechanisms and consistent language should be developed and implemented across HHR agencies where appropriate to request consent for data sharing in order to provide more assurances to citizens that information about them will not be used in ways they do not agree with. In addition, when data is shared non-disclosure and confidentiality assurances are needed from anyone who will have access to the data. Cross-agency data sharing should be accompanied with non-disclosure agreements that have specific language specifying the allowed uses of the data and consequences to the individual of disclosing or releasing the data to unauthorized users.

3 - It is widely recognized that there is significant overlap in populations served and cross-agency dependencies in delivery of services. Since the law does not provide blanket approval to share data for any purpose, the key to making programmatic improvements is to identify specific business functions and use cases within HHR that could be improved with shared data or data services. HHR agencies would benefit by having a guidance document that describes classes of uses cases that are permissible and under what type of agreement. For example, HIPAA considers all of the following to be permissible uses of identifiable data when shared under HIPAA regulations:

- Determining eligibility,
- Managing enrollment information
- Providing services,
- Ensuring accurate payment,

- Identifying and investigating fraud and abuse,
- Policy analysis,
- Program evaluation,
- Performance monitoring, and
- Outcome measurement

4 - An enhanced memorandum of agreement (eMOU) was developed by the Office of the Secretary of Health and Human Resources in 2013. It was intended to simplify the process for requesting and processing cross-agency data requests and was used by a few agencies. The eMOU requires some updating and revision to make it comprehensive enough to be used as a standard form for all cross-agency data sharing requests. It should become the basis for multi-party data sharing between HHR and other state or local agencies outside of HHR. Revisions and enhancements to the eMOU are needed to clarify purpose and constraints, definition and description of metadata, data records to be provided, and the method that will be used to exchange data.

The updated eMOU should also be used to facilitate the necessary bi-directional exchange of information with localities and between localities, as localities require state data and vice versa. Citizens are mobile. Communication and coordination are necessary between localities for services that are provided today.

5 - HB2457 allows the Secretary of Health and Human Resources to request agencies within the Secretariat to share data as long as federal law permits it. However, it is federal law such as the Federal Privacy Act, the Social Security Act, and U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), that most often is the reason state HHR agencies are not able to share data.

While Federal law regulating sharing of personally identifiable data is generally very restrictive, there are allowed exceptions and methods that can be used to enable state agencies to share sensitive data without violating federal law. For example, HIPAA allows a business associates agreement which is a contract between a HIPAA-covered entity and a HIPAA business associate (BA). The contract protects personal health information (PHI) in accordance with HIPAA guidelines. In accordance with the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, a BA's disclosure, handling and use of personal health information (PHI) must comply with HIPAA Security Rule and HIPAA Privacy Rule mandates. Under the HITECH Act, any HIPAA business associate can be held accountable for a data breach and penalized for noncompliance.

Examples of HIPAA business associates include:

- When a health plan uses a third-party administrator to help with claims processing.
- If a CPA firm provides accounting services to a healthcare provider and they have access to protected health information.
- When a hospital has a consultant perform utilization reviews.
- When a healthcare clearinghouse translates a claim from a nonstandard format to a standard format for a healthcare provider then sends the process transaction to a payer.

- When a physician uses an independent medical transcriptionist's services.
- When a pharmacy benefits manager managed a health plan's pharmacist network.

The rationale for the BA agreement is as follows. According to the Department of Health and Human Services (HHS), the HIPAA Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers. However, most health care providers and health plans do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule allows covered providers and health plans to disclose protected health information to these "business associates" if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule. Covered entities may disclose protected health information to an entity in its role as a business associate only to help the covered entity carry out its health care functions – not for the business associate's independent use or purposes

Hence, BA agreements could also be used to allow sharing data for purposes defined in HB2457 which aim to improve operations and services within the HHR secretariat. A set of BA agreements could be developed that define specific classes of data use that HHR agencies (and perhaps other entities working with HHR agencies) could utilize to authorize the sharing of data and remain in compliance with HIPAA. Each data request would still need to be reviewed to determine whether it conforms with the definitions of one of the BA agreements, but this approach may be a viable option to achieve the intended results as directed in HB2457.

The BA agreement is a written, signed agreement between the covered entity and the business associate. According to HHS, HIPAA business associate contracts should contain the following:

- Describe how the business associate is permitted and required to use PHI.
- Require that the business associate not use or disclose PHI other than as specified in the contract or as required by law.
- Require the business associate to use appropriate safeguards to ensure the PHI is used as detailed in the contract.
- The covered entity is required to take reasonable steps to cure any breach by the HIPAA business associate if and when they know of one. If this is unsuccessful, the covered entity is required to terminate the contract with the business associate.
- If contract termination is impossible, the HIPAA covered entity must report the event to the HHS Office of Civil Rights (OCR).
- A covered entity is required to report to the HHS OCR if there is a problem in terminating the contract with the business associate.

A BA agreement is not required for the collection and sharing of protected health information between a health plan that is a public benefits program, such as Medicaid, and another agency administering the

health plan, such as DSS, that collects protected data to determine eligibility or enrollment for the program where the joint activities are authorized by law.

6 - The General Assembly should leverage investments in technology where possible to facilitate identity management and data sharing for all state agencies, including enterprise level analytics as a service (modeled after programs in South Carolina and Washington State). This change would provide savings to the state through economies of scale, and Virginia may realize additional benefits by utilizing 90/10 match funding from federal agencies to pay for technology investments.

7 - The General Assembly could require all state agencies to develop formal data governance policies and processes. To further the goals of HB2457, data governance should be organized and coordinated across agencies within the HHR secretariat. This would require staff augmentation with specific expertise and responsibility in:

a) Development and coordination of data security and management policies;

b) Development and use of shared standards and common technology architecture for identity matching, finance, and procurement;

c) Development of data dictionaries, metadata and other information about the data within each agency, including any restrictions that may exist on the use and sharing of specific data elements;

d) Improvement of data quality;

e) Integration of data across different source systems;

f) Development and adoption of data classification standards across agencies;

g) Assist agencies in developing useful open data platforms for information that should be in the public domain: and

h) Encourage a culture or data stewardship and collective ownership for the public benefit.

8 - The General Assembly should consider funding the on-boarding and maintenance of the Virginia Longitudinal Data System (VLDS) to enhance broad-based evaluation of program effectiveness. VLDS is a Virginia owned and developed technology that allows agencies to link, match and share individual-level data without revealing the identity of the individual. SCHEV is the fiscal agent for VLDS. The VLDS is a technology already in place and being used by nine state agencies to share de-identified. It was designed to support several of the functions listed above, including policy analysis, program evaluation, performance, and outcomes measurement.