Secretary of Health and Human Resources and Secretary of Technology

Secretarial Committee on Data Sharing

Committee Report and Recommendations

Version 2.2

March 2012

Participating Agency Review

Participating Agency	Review Date	Agency Contact

Table of Contents

Summary

In August 2011, the Secretary of Health and Human Resources (HHR), William A. Hazel, Jr., M.D., and the Secretary of Technology, James D. Duffey, Jr., formed the Secretarial Committee on Data Sharing (SCDS). The SCDS consisted of representatives from HHR and other Commonwealth of Virginia (COV) agencies, including the Department of Motor Vehicles (DMV), Department of Education (DOE), Auditor of Public Accounts (APA), Virginia Information Technologies Agency (VITA) and Office of the Attorney General (OAG). A complete list of SCDS participants has been referenced in this report as **Appendix A**.

The SCDS mission centered on identifying opportunities and constraints for an enterprise data-sharing agreement and recommending action steps needed to establish such an agreement for participating COV agencies. A major goal of the SCDS was to align the Commonwealth with the enterprise information-sharing outcomes codified in the American Recovery and Reinvestment Act (ARRA), the Patient Protection and Affordable Care Act (PPACA) and the Medicaid information technology targets through 2014.[1] The SCDS also worked to support the goals and objectives of the Commonwealth's Information Technology Strategic Plan.[2]

Committee Objectives

The mission of the SCDS originally involved achievement of the following objectives:

- Objective 1: To identify any regulatory/code/policy constraints that needs to be addressed to facilitate the sharing of data between the entities of the Commonwealth.

- Objective 2: To make recommendations toward the creation of an enterprise data sharing agreement for the Commonwealth of Virginia.

- Objective 3: To make recommendations on changes to existing security and privacy policies and procedures to include a data use agreement for Virginia citizens, which could be incorporated into all state program user applications (for example, to support the process when a member of the public applies for any HHR program or for a driving license through the state DMV).

[1] Details on Federal health information technology initiatives can be accessed through the Office of the National Coordinator for Health Information Technology at http://healthit.hhs.gov

[2] For information on the Commonwealth of Virginia's Information Technology Strategic Plan, visit http://www.vita.virginia.gov/library/default.aspx?id=829

However, after the first meeting in September 2011, the SCDS recognized that although changes to existing security and privacy policies and procedures targeted in Objective 3 may be necessary, the Commonwealth would need to take into account the applicable laws impacting data sharing by participating agencies. The SCDS also determined that any data-sharing agreement for the Commonwealth would need to be founded on a solid trust framework and agreed to explore the Federal Data Use and Reciprocal Support Agreement (DURSA) as a guide in its deliberations.

The SCDS met monthly from September - December 2011, with each meeting targeting a specific dimension of data sharing. SCDS participants came to see the Commonwealth's data inventory as an enterprise asset, which may be used to enhance governmental efficiency, effectiveness, accountability and performance. However, the SCDS also recognized the necessity of forming an interagency trust framework as the basis of enterprise data sharing for COV agencies.

As the meetings progressed, SCDS participants realized the value of enterprise data sharing but saw that a myriad of security, privacy, business and technical constraints would need to be addressed in order for data sharing to become a reality within the Commonwealth. SCDS participants also understood that enterprise data sharing would only be possible if driven by executive-level action; articulated through enterprise data-sharing policies, standards, guidelines and procedures; and administered by a governance committee consisting of representatives from participating agencies.

Committee Recommendations

Based on its findings from participant input and staff research, the SCDS formulated the following recommendations for Secretarial consideration and action:

Recommendation 1: Issue an executive-level directive to COV agencies to establish a trust-agreement framework in support of enterprise data sharing.

Recommendation 2: Form a governance committee of executive staff, data owners, data stewards, business leads, technical leads, legal staff, security staff and other representatives from COV agencies to develop, implement and maintain a trust-agreement framework for the Commonwealth.

Recommendation 3: Identify applicable legal, regulatory and policy constraints impacting data sharing and orient the trust-agreement framework to comply with applicable requirements.

Recommendation 4: Identify legal requirements for informed consent and authorization and design the trust-agreement framework to comply with these requirements.

Recommendation 5: Develop policies, standards, guidelines and procedures to govern the operations, onboarding, maintenance, breach resolution and certification processes associated with the implementation of the trust-agreement framework.

The purpose of this report is to provide a high-level analysis of the SCDS recommendations. For each recommendation, the report offers an overview of the SCDS findings and references support documentation associated with the findings. The report also builds upon highlights from best practices, case study experience and current implementations of enterprise data sharing at the Federal, State and local level.

Analysis

Recommendation 1: Issue an executive-level directive to COV agencies to establish a trust-agreement framework in support of enterprise data sharing.

The SCDS recognized the need for executive-level action as a driver for enterprise data sharing. In its review of existing information-exchange models, the SCDS found that most had been initiated or directed by executive order or comparable action. Examples included the Nationwide Health Information Network (NwHIN), facilitated by the Office of the National Coordinator (ONC) for Health Information Technology, U.S. Department of Health and Human Services;[3] and the North Carolina Healthcare Information and Communications Alliance (NCHICA).[4] Both of these initiatives had as catalysts executive orders from the governing administrations.[5]

The SCDS found that, in the cases examined, executive action became the basis of trust agreements, which in turn established the required legal framework for the data-sharing relationships. For NwHIN, the trust framework was formalized in the Federal Data Use and Reciprocal Support Agreement or DURSA.[6] A copy of the DURSA has been referenced in this report as **Appendix B**. Steven D. Gravely, J.D., M.H.A., from the law firm of Troutman Sanders, an author of the Federal DURSA, presented to the SCDS on November 8, 2011. Mr. Gravely's presentation has been referenced in this report as **Appendix C**.

The Federal DURSA constituted a legal agreement to promote and establish trust among the DURSA signatories, referred to as "Participants." The DURSA codified a set of trust expectations into an enforceable legal framework and eliminated the need for point-to-point agreements. Rather than supplant existing law, the Federal DURSA built upon the legal requirements faced by Participants and described the mutual responsibilities, obligations and expectations of Participants under the trust agreement.

According to the DURSA,[7] the primary components of a trust framework include:

- Requirements and expectations under the agreement
- Defined standards for identity and authentication

[3] For more information on the Nationwide Health Information Network (NwHIN), visit http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__onc/1200

[4] For details on the North Carolina Health Information and Communications Alliance (NCHICA), visit http://www.nchica.org

[5] The ONC was established by Pres. George W. Bush in 2004 under Executive Order 13335: http://georgewbush-whitehouse.archives.gov/news/releases/2004/04/20040427-4.html The North Carolina Healthcare Information and Communications Alliance (NCHICA) was established in 1994 by Gov. James B. Hunt, Jr., under Executive Order 54: http://www.nchica.org/About/CorpInfo/ExecOrder.htm

[6] For an overview of the Federal DURSA and links to current versions, visit http://www.nationalehealth.org/dursa

[7] Gravely, Steven D. 2011. "Universal Components of Trust." *DURSA Overview for the Secretarial Committee on Data Sharing*, Presentation November 8, 2011, p. 3.

- Transparent oversight and governance
- Accountability and enforcement
- Technical requirements and specifications

Several key provisions of the Federal DURSA resonated with SCDS members. First, the DURSA reflected a consensus among Participants – which included Federal, State and local members – on how the trust framework would address the following issues:

- Participant obligations, responsibilities and expectations
- Privacy and security obligations
- Requests for information based on a permitted purpose
- Participants duty to respond to information requests
- Future use of data received from another Participant
- Respective duties of submitting and receiving Participants
- Autonomy principle for secure access
- Use of authorizations to support requests for data
- Participant breach notification
- Mandatory non-binding dispute resolution
- Allocation of liability risk

Second, the DURSA contained both high-level expectations and detailed operational-level policies, procedures and guidelines for implementing the trust agreement. Third, the DURSA established a governance framework led by a coordinating committee and a technical committee to document how the agreement would be implemented, maintained and updated. These provisions offered a valuable model for the SCDS to consider when framing its recommendation.

At the State level, several jurisdictions have developed trust agreements modeled on or consistent with the Federal DURSA. The Statewide Health Information Network for New York (SHIN-NY) features a trust framework defined through a Statewide Collaborative Process and implemented through Regional Health Information Offices or RHIOs.[8] Similarly, the State of Maryland's Health Information Exchange (HIE) – the Chesapeake Regional Information System for our Patients (CRISP) – operates under a universal data-sharing agreement governed by participating organizations. The trust framework was established in response to a directive from the State legislature and Gov. Martin O'Malley.[9]

Locally, MedVirginia was among the nation's first community-based HIEs and is a certified Participant in NwHIN. MedVirginia began in 2000 and has grown to offer an array of clinical information exchange services, such as a community repository of clinical data,

[8] For more information on the Statewide Health Information Network for New York (SHIN-NY), and its Statewide Collaborative Process, visit http://www.nyehealth.org/index.php/programs/statewide-collaboration-process

[9] For information on the State of Maryland Health Information Exchange – The Chesapeake Regional Information System for our Patients (CRISP) – visit: http://www.crisphealth.org

patient scheduling, e-prescriptions, electronic diagnostic test reporting and cost-effective options for electronic health records. MedVirginia's HIE operations started in 2006, and in 2009 it became the first HIE to exchange "live" patient data across the NwHIN. As a Participant in NwHIN, MedVirginia maintains a trust framework consistent with the Federal DURSA and participates in efforts of the DURSA coordinating committee.[10]

Research conducted by SCDS members documented the importance of executive-action in forming a trust framework. For example, NASCIO's guidance on enterprise data sharing cited "the full understanding and support of the state CIO, endorsement and participation by agency executives, and the backing of the current state administration and general assemblies" as key ingredients for successful data-sharing agreements. NASCIO also advised that a "lack of senior-level sponsorship" remained a principal barrier to enterprise data governance.[11]

Therefore, the SCDS recommendation for executive action to establish a trust framework for enterprise data sharing builds upon lessons learned at the Federal, State and local level. It reflects the experience of the Federal DURSA as the trust agreement supporting NwHIN, as well as the array of State- and local-level HIEs modeled on or consistent with the Federal DURSA. The SCDS recommendation also is consistent with NASCIO best-practice guidance.

Recommendation 2: Form a governance committee of executive staff, data owners, data stewards, business leads, technical leads, legal staff, security staff and other representatives from COV agencies to develop, implement and maintain a trust-agreement framework for the Commonwealth.

In formulating its recommendation for a trust framework, the SCDS recognized that the development, implementation and maintenance of such an agreement would need to be driven by a governance committee comprised of representatives from across COV agencies. Executive action was seen as a necessary factor to initiate or enable the framework, but a governance committee would be required to put the trust agreement into place and oversee its maintenance. The SCDS found that the "ownership" of a trust framework for the Commonwealth should not lie with any single agency but within a governance partnership among participants.

A comprehensive description of roles and responsibilities performed by enterprise data-sharing committees is beyond the scope of this report. However, based on the experience of the Federal DURSA, the SCDS identified several of the DURSA coordinating committee's roles as important for consideration:

- Building consensus for the trust agreement among Participants
- Identifying security, privacy and legal constraints in applicable law

[10] Details on the MedVirginia HIE and a copy of its security and privacy policies can be found at http://www.medvirginia.com/

[11] National Association of State Chief Information Officers (NASCIO), *Data Governance – Managing Information as an Enterprise Asset*, April 2008, p. 6.

- Establishing operating policies, procedures and service-level agreements
- Defining processes for onboarding, suspension and termination of Participants
- Determining the processes and procedures for breach notification
- Developing mechanisms for dispute resolution
- Managing amendments to the trust agreement

The Federal DURSA coordinating committee consists of representatives from each of the charter Participants (Federal and non-Federal), one representative from ONC and one representative selected by each Affiliation group. The committee's composition, governing authority, committee structure and other provisions are fully articulated in the DURSA, which establishes the governance body at the heart of the trust agreement.

State-level implementations modeled on or consistent with the Federal DURSA feature comparable governance committee frameworks. For example, the Maryland CRISP HIE is governed by a Board of Advisors and a Policy Board, which consists of representatives from across participating State government, health, nongovernmental and other stakeholder agencies. North Carolina's NCHICA, which is a certified NwHIN Participant, takes its direction from a governance committee framework agreed upon by its 235 organizational members.[12]

The SCDS learned from the experience from the Federal DURSA and State-level implementations as it framed its recommendation. Given the federated system of Cabinet agencies within the Commonwealth, the SCDS found that a governance framework modeled on the Federal and cited State examples would be the most appropriate for the development, implementation and maintenance of a Commonwealth trust agreement. With membership from across participating COV agencies, the governance committee would serve as the central governance body for a Commonwealth trust framework.

Recommendation 3: Identify applicable legal, regulatory and policy constraints impacting data sharing and orient the trust-agreement framework to comply with applicable requirements.

During its October 2011 meeting, the SCDS heard presentations from COV agency data owners and data stewards regarding source data systems and various formal constraints to sharing data. Some of the agency concerns included the following:

- The overall state of information security across COV agencies has improved in past years; however, security will continue to be a central concern for data sharing.
- Specific levels of accountability for data/security breaches need to be more fully defined and control responsibilities assigned in order to address concerns relating to vulnerability and trust.

[12] For information on the North Carolina Health Care Information and Communications Alliance (NCHICA), and its tool kit for data sharing, visit http://www.nchica.org/About/toolkit.htm

- Current data sharing among COV agencies tends to be *ad hoc* and limited to the program level. Opportunities for further sharing face constraints in the absence of a systematic structure to control the data-sharing process.
- Data storage and maintenance constraints, such as those posed by legacy systems, limit the capacity for enterprise data sharing. Similar storage and maintenance considerations, including data integrity, quality, reliability and disaster recovery, were cited as additional constraints.
- Managing the complexity of proliferating point-to-point data-sharing agreements presents barriers for COV agencies and their partners.

In terms of the formal rules, several agencies reported maintaining data "comingled" with Federal Tax Information (FTI), which is regulated by Internal Revenue Service (IRS) Publication 1075.[13] Other data systems included protected health information (PHI), which is covered by privacy rules under the Health Insurance Portability and Accountability Act (HIPAA)(45 CFR Part 160 and Subparts A and E of Part 164).[14] The SCDS recognized that these are just two of the many formal regulatory constraints faced by COV agencies and that a Commonwealth data-sharing agreement would need to support agency compliance with all legal and regulatory requirements.

The Federal DURSA accomplishes this through its recognition of "Applicable Law," which it defines as follows:

> (i) for the Participants that are not Federal Participants, all applicable statutes and regulations of the State(s) or jurisdiction(s) in which the Participant operates, as well as all applicable Federal statutes, regulations, standards and policy requirements; (ii) for the Federal Participants, all applicable Federal statutes, regulations, standards and policy requirements.

The SCDS recognized that "Applicable Law" for a Commonwealth trust agreement would entail governing provisions in the *Code of Virginia*, as well as other Commonwealth regulations, and all applicable Federal statutes, regulations, standards and policy requirements. A trust framework for the Commonwealth would not supplant applicable laws but would ensure compliance with codified security, privacy and related protections through the legal, policy and procedural provisions of the agreement.

The SCDS found that an important first step toward a Commonwealth trust framework would be for participating COV agencies, through engagement with OAG, to make determinations on the applicable laws and shape the trust framework to comply with these laws, or to become the driver to changes in applicable law. Key participants in this process would be the executive staff, legal staff, data owners, data stewards, business leads, technical leads, subject-matter experts and other representatives from participating COV

[13] Internal Revenue Service, Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*, http://www.irs.gov/pub/irs-pdf/p1075.pdf

[14] For information regarding the HIPAA Privacy Rule, visit http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

agencies. Oversight of this process and its implementation in the trust framework may reside with the governance committee, proposed in Recommendation 2.

Recommendation 4: Identify legal requirements for informed consent and authorization and design the trust-agreement framework to comply with these requirements.

The legal basis of informed consent, authorization and agency requirements for the collection and dissemination of personal/patient information has been established in Federal law and the *Code of Virginia*.[15] The guiding principles are codified in explicit legal provisions detailing what information may be collected or shared by COV agencies and the authorizations required to enable sharing of client/patient information. The SCDS acknowledged these provisions and recognized that a Commonwealth trust-agreement framework would need to comply with applicable laws for informed consent and authorization.

The Federal DURSA and State-level implementations take different routes for meeting informed consent and authorization requirements. The Federal DURSA places the burden of compliance on Participants, making compliance with applicable law a condition of participation rather than defining a mechanism in the trust agreement.[16] At the State level, the trust agreements often spell out the specific requirements for informed consent and authorization. The SHIN-NY, for example, mandates that participants use a pre-defined consent and authorization form, referred to as the Approved Consent Form, which has been established by the New York Department of Health.[17]

On the public-facing side of the data exchanges, jurisdictions may use an "opt-in" or "opt-out" method of client/patient enrollment to support legal consent and authorization requirements. These may not constitute replacements for the legal consent or authorization document, which may be submitted with a "wet" signature or electronically through user authentication, but they serve as a mechanism for informing the user of the data exchange and provide a choice for enrollment. For example, the Maryland CRISP HIE is an "opt-in" system, meaning that patients have to elect to enroll for their records to be shared among participating HIE providers.

The SCDS concluded that a Commonwealth data-sharing agreement would need to reflect and fully articulate informed-consent and authorization requirements. First, this would need to be part of the determination of applicable law outlined in Recommendation 3.

---

[15] For example, some of the primary governing provisions in the *Code of Virginia* include § 32.1-162.18. Informed consent; § 32.1-127.1:03. Health records privacy; and § 2.2-3800 et seq. (Chapter 38 - Government Data Collection and Dissemination Practices Act).

[16] Gravely, Steven D. 2011. "Universal Components of Trust." *DURSA Overview for the Secretarial Committee on Data Sharing*, Presentation November 8, 2011, p. 14.

[17] State of New York eHealth Collaborative 2009. *The Statewide Collaboration Process: Privacy and Security Policies and Procedures for RHIOs and their Participants in New York State*, Version 1.1: http://www.ehealth4ny.org/dl/Privacy-and-Security-Policies-and-Procedures-for-RHIO-in-NYS--V1.pdf

Second, the governance committee and participating agencies would need to decide whether using legacy consent forms would be sufficient or if a new, enterprise form would be most appropriate. Third, the formal requirements for consent and authorization would need to be clearly stated in the operational policies, procedures, guidelines and implementation instruments of the data-sharing trust agreement.

Recommendation 5: Develop policies, standards, guidelines and procedures to govern the operations, onboarding, maintenance, breach resolution and certification processes associated with the implementation of the trust-agreement framework.

The SCDS through its review of the Federal DURSA, as well as State and local-level implementations modeled on or consistent with the DURSA, found that a trust-agreement framework for the Commonwealth would need to be clearly defined in policies, standards, guidelines and procedures (PSG&Ps). Given the array of business rules, technical specifications and security and privacy constraints on source data systems, the SCDS realized that defining the PSG&Ps would need to be a collaborative process among participating COV agencies. Central to this role would be the data owners, data stewards, business leads, technical leads, subject-matter experts and other agency stakeholders.

Some of the primary areas to be covered by the PSG&Ps include:

- Organizational and Governance Structure
- Participant Onboarding and Certification
- Data Governance and Standards
- Data Quality and Integrity
- Data Security and Privacy Requirements
- Informed Consent and Authorization
- Permitted Purposes
- Participant Authentication
- Operating Policies, Procedures and Service-Level Agreements
- Performance and Service Specifications
- Technical and Business Requirements
- Participant Training on Data Sharing and Use Restrictions
- Breach Reporting
- Dispute Resolution
- Participant Suspension and Termination

The SCDS recommended that the definition, development and vetting of these PSG&Ps consist of an iterative engagement process among the participating COV agencies. Ownership of the process, as well as the ongoing maintenance and updates to the PSG&Ps, also should be collaborative and reside with the governance committee of the trust-agreement framework.

The process of defining, developing and vetting the PSG&Ps recommended by the SCDS is consistent with the process used for the Federal DURSA and State-level implementations. Participants in the Federal DURSA engaged in an 18-month process from May 2008, when a test DURSA was developed and routed for review, through November 2009 when an executable version of the DURSA was approved by NwHIN. The most recent update to the DURSA overseen by the coordinating committee was approved in May 2011. The SHIN-NY followed a comparable path, and updates to its operating policies and procedures are governed under the Statewide Collaborative Process.

Conclusions

The SCDS participants viewed data maintained by COV agencies as an enterprise asset, one that may be used to inform strategies for enhancing governmental efficiency, effectiveness, accountability and performance. The SCDS realized that sharing of data across the enterprise would need to be driven by executive action and facilitated by a trust-agreement framework. Most importantly, the SCDS recognized the public trust underlying the collection, maintenance and dissemination of data and stressed that the trust-agreement framework should serve to reinforce the public's trust.

The lessons learned through the experience of the Federal DURSA and State-level implementations modeled on or consistent with the DURSA will provide valuable insight to the Commonwealth as it proceeds with establishing a trust-agreement framework. However, the final trust agreement will need to be formulated, fully vetted and tested prior to the Commonwealth's adoption. Formulating and maintaining a trust-agreement framework will take time and needs to be driven by an iterative, collaborative process among COV agencies. Through each iteration, participants must maintain close engagement at all levels of governance.

Appendices

Appendix A. List of Participants on the Secretarial Committee on Data Sharing.

Available at
http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/EAD/Enterprise_Data_Management/AppendixA_SCDS_Participants_List.pdf

Appendix B. Restatement I of the Federal Data Use and Reciprocal Support Agreement (DURSA), Version Date: May 3, 2011.

Available at
http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/EAD/Enterprise_Data_Management/AppendixB_Restatement_I_DURSA.pdf

Appendix C. PowerPoint Presentation. Gravely, Steven D., J.D., M.H.A. *DURSA Overview for Secretarial Committee on Data Sharing*, Presented on November 8, 2011.

Available at
http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/EAD/Enterprise_Data_Management/AppendixC_DURSA_overview.pdf