Kentucky Health Data Trust Initiative

Key Elements of Data Security Policies and Procedures

Deliverable 4.3.4

Prepared for the Kentucky Health Data Trust
Interagency Governance Workgroup

Freedman HealthCare
July 30, 2015

Freedman
HEALTHCARE

Introduction

Establishing a strong data security framework is a critical function of an APCD's data governance structure. Robust security policies and procedures address privacy concerns of data owners and other stakeholders, as well as protect the APCD from security breaches and other threats. The purpose of this document is to provide CHFS and its partners with a starting point for building a security framework for the Kentucky Health Data Trust (KyHDT). This is not a comprehensive list of security policies and procedures; rather, this document outlines best practices and lessons learned for APCD data security.

Key Assumptions about APCD Security

- The APCD infrastructure will be HIPAA and HITECH compliant – the minimum standard for health data initiatives.
- A comprehensive set of security/privacy rules will be in place to protect data during transmission, storage, and release.
- Role-based permissions allow designated users to access the data warehouse and BI tool. As needed, these security authorizations are adjusted to permit a user to access specific subject datasets, fields, and tables within the APCD environment.
- Public-facing information, extracts, or reports from the APCD will never include protected health information (PHI).

Minimum Security Requirements for Data Intake and Storage

- All communication between the APCD and the data submitters (in both directions) are encrypted in motion and at rest.
- Only a pre-approved, credentialed list of data submitters and their unique IP addresses can send data to the secure APCD server. One option for this process would be PGP encryption, in which senders and recipients exchange keys to confirm their identities.
  - *APCDs require data submitters to register prior to submitting files.*
  - *APCDs also require use of a particular data submission encryption package, often supplied by the APCD data security manager. (See examples from Massachusetts, Minnesota and Colorado below.)*
- The APCD team conducts security audits on an established schedule to test the security of the APCD server.
  - *Audits and penetration testing are emerging as necessary components of the APCD security infrastructure. The federal Qualified Entity Certification Program has prepared a thorough inventory of security structures, policies and procedures deemed necessary to protect identified Medicare data files. This inventory could serve as a template for APCDs, even those that are not planning to become qualified entities. (For more information, see page 18 and Appendix D in the QECP Operations Manual and the Security and Privacy Controls put forth by the National Institute of Standards and Technology.)*
- The data warehouse ensures that identifiable data is available only to approved users.
  - *User profiles should be standardized to minimize customization and ensure appropriate updates. This technology is still emerging in APCD environments, and is more common in enterprise-wide State agency data warehouses.*
- Assignment of a Master Patient Identifier (MPI) takes place in a secure environment that is separate from the APCD's data production environment.
  - *An MPI greatly enhances the utility and credibility of the database as well as creating an opportunity to remove certain direct identifiers (CO, RI).*

- Access to the data warehouse is available to properly trained individuals whom the data owners have authorized. The APCD infrastructure is flexible enough to allow access to as many authorized users as necessary. Some areas of the data warehouse containing only de-identified data may have unlimited access, while users accessing more secure areas must first complete the proper authorization and training process.
- All authorized personnel with access to the data warehouse must sign a data use agreement.
    - *While an organization's data use agreement may cover its individual employees, experience suggests that data privacy and security are everyone's responsibility. Each user should acknowledge her/his role in protecting the data from unauthorized access and use (MA, RI).*

Lessons Learned

Build security protections early. The APCD team must design security policies and procedures that include, and build off, the state's existing policies and procedures to secure PHI and other sensitive data. To date, no state APCD has experienced a massive data breach; however, if this were to happen, it would most likely cripple the state's APCD initiative and severely impact the public perception of APCDs nationwide. Guarding against data breaches is therefore critical and requires careful planning from the earliest stages of APCD development.

Explain the privacy and security protections to a broader audience. Technical staff must work with communications experts to convey the degree and extent of the protections around the data. At least two types of materials may be needed:

- One explanation should be accessible for a technical audience familiar with state-of-the-art protections.
- The second set of materials must be accessible for a less technically literate audience. In Colorado and Arkansas, the APCDs produced two-page documents responding to questions such as "What would a hacker see?" and "How is my information protected?"(See links below).

Engage qualified data security experts. While maintaining data security is not an ongoing, day-to-day task, it is dependent on having proper security models, policies, and procedures in place from the beginning. States should appoint a data security officer to define and oversee all security processes for the APCD. This individual, or team of individuals, should be closely involved in the APCD planning process to develop and implement security policies and procedures.

Other Resources: Data Security in Other States

The following links provide a brief overview of how States have addressed data security for their APCDs.

- Colorado APCD Privacy, Security, and Data Release Fact Guide
- Arkansas APCD Data Protection
- Minnesota's All-Payer Claims Database Frequently Asked Questions – February 2015
- Overview of the Massachusetts All-Payer Claims Database – February 2015
- Colorado APCD – Frequently Asked Questions: Privacy and Security