July 13, 2007

Privacy and Security Solutions for Interoperable Health Information Exchange

Privacy and Security Assessment of Variation Toolkit

Prepared for

Jonathan White, MD, Director of Health IT
Agency for Healthcare Research and Quality
540 Gaither Road
Rockville, MD 20850

Jodi Daniel, JD, MPH, Director
Steven Posnack, MHS, MS, Program Analyst
Office of Policy and Research
Office of the National Coordinator
330 C Street SW
Switzer Building, Room 4090
Washington, DC 20201

Prepared by

Linda L. Dimitropoulos, PhD
RTI International
230 W Monroe, Suite 2100
Chicago, IL 60606

Contract No. 290-05-0015
RTI Project Number 0209825.000.004.006

RTI is grateful to the following members of the Technical Advisory Panel who have kindly given us permission to include their work as part of the toolkit:

Mr. Chris Apgar, CISSP, Apgar and Associates, LLC
Mr. John R. Christiansen, Christiansen IT Law
Mr. John C. McKenney, CIPP, SEC Associates, Inc

Contents

Overview

Background and Purpose

This toolkit provides guidance for conducting organization-level assessments of business practices, policies, and state laws that govern the privacy and security of health information exchange (HIE).

Assessing the variation in organization-level business practices enables regions, states, and territories to identify the variation in practices, policies, and laws that may present barriers to interoperable health information exchange. The assessment will help to identify specific practices that may pose challenges (eg, the requirement for a wet signature), as well as practices that facilitate interoperable exchange (eg, acceptance of digital signatures). This, in turn, will allow investigators to identify and propose practical solutions to barriers while preserving privacy and security requirements as defined by the local community and in applicable federal and state laws and will enable them to develop detailed plans for implementing solutions.

Health information exchange refers to the sharing of clinical and administrative data across the boundaries of health care institutions and other health data repositories. Many stakeholder groups (payers, patients [consumers], providers, and others) realize that if data could be more readily shared in a safe and secure manner, health care processes would improve with respect to a number of indicators including safety, quality, and cost. From a cultural and technical standpoint, sharing health data is not easy. Stakeholders have competing priorities. Financial concerns, unresolved issues related to data ownership, and privacy and security issues are among some of the hardest cultural barriers to overcome.

There is widespread agreement that there are benefits to health information exchange. Improvements in health information exchange are expected to

- improve continuity of care across health care providers;
- reduce medical errors;
- avoid costly duplicate testing;
- eliminate unnecessary hospitalizations;
- increase consumer convenience;
- provide life-saving early detection of an infectious disease outbreak, as anonymous data from emergency rooms are sent to public health systems instantly; and
- ensure that patients' health information is available when needed.

Consumers have concerns about the misuse of medical data. Media reports of compromised data raise fears of identity theft. The sensitive nature of health data could result in discrimination, inability to get a mortgage, loss of employment, or loss of insurance. These

concerns can affect behaviors, making consumers reluctant to obtain medical care or leading them to provide false or incomplete information to health care providers.

The regulatory environment surrounding health information is complex. The Health Insurance Portability and Accountability Act (HIPAA) is the federal statute that provides a baseline of protection. Privacy protections beyond the HIPAA Privacy and Security Rules are also found in federal law, common law, state law, and contracts and organization-level business practices and policies. Many states have privacy laws that exceed the provisions of the Privacy Rule in areas such as sexually transmitted diseases and reproductive health, alcohol and drug abuse, genetic information, HIV/AIDS, mental health, and child or adult abuse. Many states also have laws that address security, primarily to protect against identity theft. In addition to state laws, organizations that handle health information, both within and across states, have business policies and practices in place that add another layer of protection. In many cases, these are more protective than the HIPAA Rules.

Three basic assumptions underlie the assessment of variation:

1. It is valuable to identify best practices and solutions that have the potential to accelerate nationwide electronic health information exchange, particularly on privacy and security questions, for consideration and adoption by communities and states.
2. Health care is local and the solutions to improving health care should accommodate community variation.
3. Stakeholders at the state and community levels, including patients and consumers, must be involved in developing solutions to achieve acceptance.

The first step toward interoperability is to identify the variations in organization-level business privacy and security policies and practices and state laws that affect electronic health information exchange. The second step is to engage stakeholders in discussions where they can come to agreement on the common and necessary elements of current practices that will need to be retained and to identify gaps in current protections that are inadequate to cover the requirements for electronic health information exchange. The third step is to identify the policy or legal driver or other underlying rationale for the current practice and work toward identifying consensus-based solutions. The fourth step is to develop a plan to implement the solutions. The final step is to work through the implementation process, collaborating openly with stakeholders.

One goal of the privacy and security project was to create long-lasting collaborative networks in states and communities to support future work and inform future health information exchange activities. Following this process can also help create a knowledge base in states and communities about privacy and security issues related to electronic health information exchange.

We invite and encourage your feedback on the content, organization, and usefulness of this toolkit as we continue to expand and improve it. Please send your comments or questions about the evaluation toolkit or the National Resource Center to ResourceCenter@norc.org.

Section 1: Tools

Section 1 presents the basic tools for assessing variation in business practices, as well as materials that facilitate productive meetings with stakeholders.

1 Scenarios Guide
2 Dimensions of Business Practices
3 Data Collection Template
4 Guidelines for Describing Business Practices
5 Example Business Practices
6 Stakeholder Meeting Discussion Guide
7 Stakeholder Meeting Checklist
8 Stakeholder Meeting Debriefing Guide

1. Scenarios Guide

This document includes the text of 18 health information exchange scenarios, along with a number of suggested areas for discussion of business practices associated with each scenario. Each scenario engages multiple stakeholders and involves multiple domains of privacy and security. The scenarios were developed by the American Health Information Management Association (AHIMA) and were designed to describe different purposes for health information exchange including treatment, education, research, marketing, public health, and biosurveillance, to ensure a thorough review of all relevant business practices. The scenarios guide also includes a mapping of scenarios to stakeholder groups, to inform decisions about creating the right mix of stakeholders needed to review each scenario and generate business practices and policies consistent with each stakeholder role.

Each practice reported by stakeholders will be identified as either a barrier or not a barrier to health information exchange. Practices that are not barriers are defined broadly as those that facilitate health information exchange, are consistent with state law, permit interoperability, and are relatively easy to put into practice. Barriers are defined as "practices, policies, or laws that impede, prohibit, or impose conditions on health information exchange—without judgment at this stage regarding the degree of appropriateness of the barrier."

Identifying a practice as a barrier will flag that practice for further review and potential resolution. Legal experts should identify the policy and/or legal drivers that underlie any practice deemed a barrier to interoperability. Stakeholders should analyze the barriers and develop a range of feasible solutions to be included in implementation planning.

Implementation plans will assign responsibility for tasks, identify inputs and dependencies, organize tasks into a sequential path, define time frames for completion of stages and the plan as a whole, assess resource requirements and associated cost, identify potential funding sources, and monitor and measure performance throughout the implementation process.

2. Dimensions of Business Practices

This document defines the 9 domains of privacy and security and describes the dimensions of business practices associated with each. It also provides examples of business practices from both the paper and electronic health information environments that were reported during the pilot study.

3. Data Collection Template

This Excel file reproduces the data fields completed by state teams to provide guidance for others wishing to engage in a similar exercise. Detailed instructions for using this tool are provided in Tool 4, *Guidelines for Describing Business Practices.*

4. Guidelines for Describing Business Practices

This document provides detailed instructions for collecting complete and useful data in each of the fields found in Tool 3, *Data Collection Template*. It can help ensure that quality data are collected, so that each state can conduct a complete assessment of the variation of business practices and can produce results comparable with those obtained by the state teams.

5. Example Business Practices

The examples provided here demonstrate the principles described in Tool 4, *Guidelines for Describing Business Practices*. The top two rows in the example spreadsheet, "Description of Data Item" and "Specific Notes and Comments," provide additional explanations of each data item and the processes by which they may be collected.

6. Stakeholder Meeting Discussion Guide

This guide was developed to enable users to reproduce the process used by the state teams. The guide is to be used by meeting facilitators to elicit business practices and their drivers (policies and laws) relevant to the scenarios. Participants should be encouraged to indicate whether a particular practice is a barrier to information exchange, assists in information exchange, or is neutral in that regard. Practices can originate from organizational business decisions, as well as from state and federal laws. Additionally, since this exercise is not intended to pass judgment on particular business practices, every effort should be made to maintain objectivity toward all participants.

Facilitators do not need to be conversant with the details regarding the exchange of identifiable patient information; however, they should be somewhat familiar with the HIPAA Rules. State laws that are more protective than HIPAA preempt HIPAA; thus, states can and do have requirements that go above and beyond provisions of the HIPAA Rules. Finally, some health care entities make business decisions to pursue certain practices that are not required by law. This knowledge will become important when probing for details during the group meetings.

7. Stakeholder Meeting Checklist

This document details the preparation procedures for facilitators of the stakeholder meeting discussion.

8. Stakeholder Meeting Debriefing Guide

Debriefing should happen immediately after the stakeholder meeting facilitation. Effective debriefing relies on a strong and honest relationship where the facilitators can comment on the parts of the facilitation that went well, the parts that did not, and what changes could be made for the next meeting. This could be particularly important if facilitators are conducting multiple meetings throughout a state or territory. In this way, the facilitator is continually improving his or her skills. This document provides a guide to addressing the critical components of the facilitation exercise.

Section 2: Reference Materials

A Reference Library

B Existing Guidance to Support HIE Implementation Opportunities

C Relevant Legal Requirements for Health Data Exchange for Health Care Organizations

D IT Privacy and Security Primer

E Glossary

A. Reference Library

This document was created by the privacy and security project's Technical Advisory Panel as background material and was provided to state teams as part of their Manual of Operations. It includes references to relevant Department of Health and Human Services publications and to other public and private organization publications.

B. Existing Guidance to Support HIE Implementation Opportunities

There is an important opportunity for states and territories to advance their own implementation strategies and simultaneously help ensure that they do not deviate too far from each other. While it is necessary and appropriate for states and territories to implement solutions suitable for their own circumstances, inconsistent solutions in key areas that are necessary for effective health information exchange may raise new barriers to

interstate activities and transactions. Reference to and use of nationally recognized guidance to support implementation should help minimize the risk of this kind of inconsistent development.

C. Relevant Legal Requirements for Health Data Exchange for Health Care Organizations

This document was written by John R. Christiansen of Christiansen IT Law in his capacity as a member of the Technical Advisory Panel as an appendix to the Manual of Operations. It provides basic information about key legal issues affecting health information sharing.

D. IT Privacy and Security Primer

This document was written by three members of the Technical Advisory Panel: Chris Apgar, Apgar and Associates; John C. McKenney, SEC Associates; and Neil McClenney, SEC Associates. It was originally distributed to project participants as an appendix to the Manual of Operations and provides helpful background discussions of fundamental IT issues necessary for understanding the technical controls that ensure privacy and security in health information exchange environments.

E. Glossary

This document was compiled as a companion to reference materials C and D, to ensure consistent understanding of the terms used. It was originally distributed to project participants as an appendix to the Manual of Operations and serves as a useful guide to key concepts in the area of electronic health information exchange.