



## Managing Information Privacy & Security in Healthcare

### Privacy and Security Solutions for Interoperable Health Information Exchange (also known as the HISPC project)

By John C. McKenney, CIPP

#### Background

On April 27, 2004, the President issued an executive order announcing his commitment to the use of health information technology (health IT) to reduce medical errors, lower costs, and provide better information for consumers and physicians. In particular, the President called for the widespread adoption of electronic health records (EHRs) and for health information to follow patients throughout their care in a seamless and secure manner. Widespread use of EHRs offers a unique means of improving quality, lowering health care costs, and preventing medical errors, which may contribute to the death of between 50,000 and 100,000 Americans per year.

The executive order directed the Secretary of Health and Human Services (HHS) to establish within the Office of the Secretary the Office of National Coordinator for Health Information Technology (ONC). On July 21, 2004, ONC released the Framework for Strategic Action, outlining the goals and strategies to realize the President's goal. One of the critical actions outlined in the strategy was to fund a nationwide effort to assess and develop plans to address variations in organization-level business policies and state laws that affect privacy and security practices - including those related to the Health Insurance Portability and Accountability Act (HIPAA) - and that may pose challenges to interoperable health information exchange.

The results of this initiative will play a role in the larger effort to develop the Nationwide Health Information Network (NHIN), a "network of networks," where state and regional health information exchanges and other networks that provide health information services, work together through common standards, processes, and policies to securely interchange information. The challenge in establishing the NHIN is to develop technology and business process standards that allow nationwide access and interoperability while keeping patient information secure, protecting individual patient privacy and ensuring the appropriate degree of patient control over their records.

Regulations promulgated pursuant to HIPAA established baseline health care privacy requirements for protected health information and established security requirements for electronic protected health information. Many states have adopted policies that go beyond HIPAA. The manner in which hospitals, physicians and other health care organizations implement required security and

privacy policies varies and is tailored to meet their individual organizations' needs. These variations in policies present challenges for widespread electronic health information exchange.

### The Privacy and Security Project Team is Formed

In September of 2005, RTI International (RTI) was awarded an \$11.5 million contract (which was later increased to \$17.2 million) to lead the privacy and security project. RTI, a private, nonprofit corporation, was selected to lead the program, which was officially titled "Privacy and Security Solutions for Interoperable Health Information Exchange." The Agency for Healthcare Research and Quality (AHRQ) and ONC co-manage and fund this contract.

RTI partnered with the National Governor's Association (NGA) Center for Best Practices and a multidisciplinary team of experts known as the Technical Advisory Panel (TAP). RTI also subcontracted with the American Health Information Management Association (AHIMA) and the AHRQ National Resource Center.

### The Health Information Security and Privacy Collaboration (HISPC) is Formed

In January of 2006, RTI issued a Request for Proposal which culminated with RTI awarding subcontracts to 33 U.S. states and one territory, Puerto Rico. The subcontracted states and territory are known as the Health Information Security and Privacy Collaboration (HISPC). Further references in this discussion to the HISPC states (or states) are inclusive of Puerto Rico. HISPC's goals are to:

1. Assess variation in business practices, policies and state laws that impact private and secure electronic health information exchange (eHIE)
2. Identify both effective practices as well as challenges
3. Develop feasible, consensus-based solutions for interoperable eHIE that protect the privacy and security of health information
4. Develop plans to implement solutions

The consensus-based solutions and implementation plans that are developed through this work could have far-reaching implications for all as we move toward achieving the goal of having nationwide interoperable electronic health records.

The HISPC subcontracting states and territory are: Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Florida, Iowa, Illinois, Indiana, Kansas, Kentucky, Louisiana, Massachusetts, Maine, Michigan, Minnesota, Mississippi, North Carolina, New Hampshire, New Jersey, New Mexico, New York, Ohio, Oklahoma, Oregon, Puerto Rico, Rhode Island, Utah, Vermont, Washington, Wisconsin, West Virginia, and Wyoming. See: [healthit.ahrq.gov/privacyandsecurity](http://healthit.ahrq.gov/privacyandsecurity) for more information about each participating state.

### Stakeholder Involvement

There is only one subcontracted organization per HISPC state, and each subcontracted entity was designated by the governor of that state. Each state identified a steering committee that is a

private-public partnership composed of leaders from state government and stakeholder organizations, and all work is conducted through a series of coordinated work groups with specific charges. The HISPC states have reached out to a broad range of stakeholders including:

- providers
- payers
- federal health facilities
- state government
- hospitals
- public health agencies
- community clinics and health centers
- laboratories
- pharmacies
- long-term care facilities and nursing homes
- homecare and hospice
- correctional facilities
- professional associations and societies
- medical and public health schools that undertake research
- quality improvement organizations
- consumers and consumer organizations

Subcontractors have been working with health care providers, consumers, payers, and many other stakeholders in their states and territories to address privacy and security issues and to identify solutions for broad application. This includes identifying variations in privacy and security practices and state laws affecting electronic clinical health information exchange (HIE); developing best practices and proposed solutions to address identified challenges; and increasing expertise about health information privacy and security protection in communities. The states are also developing implementation plans for future HIE activities, based on solutions developed over the course of the contract.

The RTI contract serves as a broad and critical initiative in support of the larger goal of electronic health information exchange. Identification of privacy and security issues under this contract, and the solutions that are ultimately crafted in response to those issues, will provide a foundation for future work by ONC and AHRQ, and facilitate health information exchange within and across states boundaries.

### **The Goals of the Privacy and Security Project**

The Privacy and Security project will play a key role in laying policy groundwork to support widespread interoperable electronic health information exchange. The assessment of variations in organization-level privacy and security practices and policies, and any related laws and regulations, will identify the practices and policies that are currently in place across a broad array of stakeholders. Practices, policies and related laws will be reviewed to assess whether the particular practice, policy, or law would pose a challenge to the electronic exchange of health information. The HISPC subcontractors will:

- Preserve privacy and security protections in a manner consistent with interoperable health information exchange
- Incorporate state and community interests, and promote stakeholder identification of practical solutions and implementation strategies through an open and transparent consensus-building process
- Leave behind in states and communities a knowledge base about privacy and security issues in electronic health information exchange that endures to inform future HIE activities

### Outcomes of the Privacy and Security Project

- Stakeholders, including state entities, will have a fuller understanding of variations in organization-level privacy and security related business practices and policies, as well as any related or underlying legal requirements in their state or territory and communities
- States, through the use of stakeholder groups, will design practical solutions and implementation plans for preserving the privacy and security protections of health information while implementing electronic health information systems
- Long-lasting collaborative networks and knowledge bases will be established in and across states and communities that will support future work

### State Teams Methodology and Organization

State teams followed a modified community-based research model that provided flexibility to each team to organize its leadership, steering committee, and work groups to ensure that the appropriate expertise and stakeholder groups were brought together. Each team was required to identify a steering committee and a number of work groups, all with a specific charge and requiring a specific core expertise. Work groups were intended to be collaborative and to have overlap in their membership.

- **Steering Committee (SC)** - The Steering Committee is a decision-making body tasked with overseeing the work of all state working groups and finalizing deliverable reports that will serve as the basis for the next steps in the process. The Steering Committee is a multi-stakeholder group that includes representatives from each stakeholder group, members of the legal working group, representatives from state government (including an individual directly representing the governor), and the state subcontractor.
- **State Variations Working Group (VWG)** - The VWG was tasked with assessing variations in organization-level business policies and practices and categorizing them as barriers, best practices, or neutral with respect to interoperability. The VWG worked closely with the state Legal Working Group to identify any legal drivers behind the policies and to produce the Interim and Final Assessment of Variation Reports.

- **State Legal Working Group (LWG)** - The LWG was tasked with reviewing the barriers uncovered in the business policy assessment (see VWG) and mapping those barriers to applicable state privacy and security laws. Members of the LWG are also working with the Solutions Working Group and the Implementation Planning Working Group to ensure that laws are accurately and consistently interpreted throughout the process of formulating solutions and planning implementation of those solutions.
- **State Solutions Working Group (SWG)** - The SWG was tasked with reviewing the assessment of variation of state laws and business policies identified as barriers by the VWG and formulating preliminary solutions to the barriers. The SWG drafted the initial and final Analysis of Solutions Reports.
- **State Implementation Plan Working Group (IPWG)** – Working from the Interim Analysis of Solutions Report, the IPWG developed preliminary implementation plans, as documented in the Interim and Final Implementation Plan Reports.

Each team followed a “core” methodology that ensured consistency across the states. The discussions were organized around 18 exchange scenarios developed and tested by AHIMA for this project. The scenarios were developed to cover 11 specific purposes for the exchange of information that were most commonly the subject of regulation and policy development. The scenarios also focused on 9 separate domains of privacy and security. This increased the likelihood that the discussions would be comprehensive.

### The Nine Domains of Privacy and Security

The analyses of organization-level business policies and practices were centered on the following nine privacy and security domains:

1. **User and entity authentication** to verify that a person or entity seeking access to electronic personal health information is who they claim to be.
2. **Information authorization and access controls** to allow access to only people or software programs that have been granted access rights to electronic personal health information.
3. **Patient and provider identification** to match identities across multiple information systems and locate electronic personal health information across enterprises.
4. **Information transmission security** or exchange protocols (encryption, etc.) for information that is being exchanged over an electronic communications network.
5. **Information protections** so that electronic personal health information cannot be improperly modified.
6. **Information audits** that record and monitor the activity of health information systems.

7. **Administrative or physical security safeguards** required to implement a comprehensive security platform for health IT.
8. **State law restrictions** about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.
9. **Information use and disclosure policies** that arise as health care entities share clinical health information electronically.

### HISPC Regional Meetings

In October and November of 2006, 10 regional meetings were held to share the work to date across states. In attendance were representatives from the HISPC states, 9 additional states, RTI, NGA, AHRQ, ONC, and the Technical Advisory Panel. The purpose of the meetings was to bring together Privacy and Security Project leaders and key stakeholders from other states to share information, discuss progress made to that point, and to encourage networking within and across state borders as a means to advance the goals of the project.

### HISPC National Conference

On March 5 and 6, 2007, more than 300 stakeholders from 42 states and Puerto Rico attended a HISPC national meeting organized by RTI. The conference, held in Bethesda, Md., provided an opportunity for members of the public, representatives from non-HISPC states, and those involved with the project to learn more about project findings to date and voice their perspectives regarding potential privacy and security solutions in electronic health data exchange.

### Summary of Key Findings/Issues from the National Conference

Differing interpretations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule among states and businesses create a wide variety of organization-level business practices across the nation.

Stakeholders expressed a lack of knowledge and significant concern related to the technologies available to protect security and privacy of individuals as well as the associated administrative processes and liabilities. In general, consumers are most concerned about privacy; providers are more concerned about liability.

Stakeholders identified a general misunderstanding regarding the many potential intersections of present state laws and HIPAA. State laws do not currently address or apply sensibly to the proposed electronic exchange of health information.

Stakeholders see a need for standards regarding the definitions, roles, functions, and funding structures of regional health information organizations. The lack of experience within organizations designed to govern electronic data exchange, and the uncertainty about their legal status, has

major implications for stakeholders seeking to design and put into practice consensus-based privacy and security solutions.

Stakeholders recognize a need to develop a system that accurately and consistently matches individual patients with their health record information, which is created and updated by various health care providers/organizations. The system must both ensure medical accuracy and protect consumers from unauthorized disclosure of personal information.

Stakeholders require a standard set of definitions and terms to develop the state and federal laws and supporting business processes to facilitate sharing of health information. For example, terms like medical emergency, current treatment, related entity, and minimum necessary do not have agreed upon definitions and therefore serve to increase variation as organizations attempt to meet compliance by defining terms in ways that protect the interests of the organization.

Stakeholders are concerned about policies that would govern the rights, responsibilities and management of health information within the proposed network. A key question is whether and/or how much access patients should have to their health information.

Other separate government-funded projects are under way to develop technology standards, product certifications, health information networks and best practices. The work under the Privacy and Security Solutions for Interoperable Health Information Exchange contract complements these other ongoing efforts.

### Summary of Session Presentations from the National Conference

For detailed information about the sessions conducted during the two days of the national meeting and the presentations at each of the sessions, [see HISPC Meeting Sessions and Presentations](#).

### Current Project Status

At the time of this writing, the HISPC states have provided all but the last of their final reports to RTI. RTI, along with the NGA and the Technical Advisory Panel, are in the process of analyzing and summarizing the final reports from the states. The contract is slated to end in June, 2007, after which AHRQ and ONC will make public the findings and final reports from RTI and the HISPC state teams.

#### The Project Team led by RTI International includes:

Linda Dimitropoulos, PhD. - Project Director

John Loft, PhD.

Barbara Massoudi, PhD,

Stephanie Rizk, MA

Robert Bailey

David Harris, MPH

Cynthia Irvin, PhD

Amoke Alakoye, MA

Alison Banger, MPH

The National Governor's Association Center for Best Practices is represented by:  
Kathleen Nolan, MPH - Director, Health Division  
Michelle Lim Warner, MPH - Senior Policy Analyst

**The Technical Advisory Panel and Subcontractors are:**

- Bill Braithwaite, MD, PhD, Health Information Policy Consulting
- John McKenney, CIPP, SEC Associates, Inc.
- Mike Hubbard, JD, Womble, Carlyle, Sandridge and Rice, PLLC
- John Christiansen, JD, Christiansen IT Law
- Chris Apgar, CISSP, Apgar & Associates
- Holt Anderson, Executive Director, NCHICA
- Ryan Bosch, MD, George Washington University
- Joy Pritts, JD, Health Policy Institute, Georgetown University
- Anna Orlova, PhD, Public Health Data Standards Consortium
- Walter Suarez, MD, MPH, Institute for HIPAA/HIT Education and Research
- Carolyn Hartley, Physicians EHR
- Gary Christoph, PhD, NCR Teradata
- AHIMA
- AHRQ National Resource Center