Privacy and Security Solutions for Interoperable Health Information Exchange

Nationwide Summary

Prepared for:

Agency for Healthcare Research and Quality
U.S. Department of Health and Human Services
540 Gaither Road
Rockville, MD 20850
www.ahrq.gov

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

Contract No.: 290-05-0015
RTI Project Number: 0209825.000.009

Prepared by:

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

AHRQ Publication No. 07-0080-3-EF
July 2007

Agency for Healthcare Research and Quality
Advancing Excellence in Health Care • www.ahrq.gov
HEALTH IT

Privacy and Security Solutions for Interoperable Health Information Exchange

Nationwide Summary

Prepared for:

Agency for Healthcare Research and Quality
U.S. Department of Health and Human Services
540 Gaither Road
Rockville, MD 20850
www.ahrq.gov

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

The authors of this report are responsible for its content. Statements in the report should not be construed as endorsement by the Agency for Healthcare Research and Quality or the U.S. Department of Health and Human Services.

RTI International is a trade name of Research Triangle Institute.

List of Authors for Summary Report

Amoke Alakoye, MHS, RTI International
Holt Anderson, Executive Director, NCHICA
Chris Apgar, CSSP, CISSP, Apgar & Associates
Alison Banger, MPH, RTI International
Ryan Bosch, MD, George Washington University Medical Faculty Associates
Robert F. Bailey, BA, RTI International
William Braithwaite, MD, PhD, Braithwaite Healthcare Consulting
John Christiansen, Christiansen IT Law
Gary Christoph, PhD, CIO, Teradata
Linda L. Dimitropoulos, PhD, RTI International
David H. Harris, MPH, RTI International
Mike Hubbard, Womble, Carlyle, Sandridge & Rice, PLLC
Cynthia L. Irvin, PhD, RTI International
John Loft, PhD, RTI International
Barbara L. Massoudi, MPH, PhD, RTI International
John McKenney, SEC Associates
Anna Orlova, Public Health Data Standards Consortium
Harry Rhodes, MBA, RHIA, CHPS, AHIMA
Stephanie Rizk, MS, RTI International
Joy Pritts, PhD, Health Policy Institute, George Washington University
Walter Suarez, MD, CEO, Institute for HIT/HIPAA Education and Research
Michelle Lim Warner, MPH, Center for Best Practices, National Governors Association

Contents

Section **Page**

Executive Summary **ES-1**

1. Scope and Purpose of the Nationwide Summary **1-1**

1.1 Description of the Scope and Purpose of this Report 1-1

1.2 Report Limitations 1-2

2. Overview of the Privacy and Security Contract **2-1**

2.1 Project Assumptions 2-1

2.2 Project Goals 2-2

2.3 Project Limitations 2-2

2.4 Limitations of Stakeholder Group Participation 2-4

3. Formation of the Health Information Security and Privacy Collaboration **3-1**

3.1 Procurement Process 3-1

3.2 Work Groups 3-1

3.3 Stakeholder Outreach 3-2

3.4 Steering Committees 3-5

4. Methodology **4-1**

4.1 Approach 4-1

4.2 Methodological Tools and Support 4-2

4.3 Process 4-3

4.4 Regional Meetings 4-5

4.5 Nationwide Meeting 4-5

5. Current Nationwide Landscape for Privacy and Security Solutions **5-1**

5.1 Overview of HIT/HIE Landscape of HISPC States 5-2

5.1.1 Single-Organization HIT Efforts 5-3

5.1.2 Local/Regional Multiorganizational HIE Efforts 5-3

5.1.3 Statewide Electronic Health Information Exchange—Early Planning 5-3

5.1.4 Statewide HIE—Establishing Foundation Components 5-4

5.1.5 Statewide HIE—Establishing Early Implementation 5-5

5.1.6 Statewide HIE—Functional/Operating Implementation 5-5

5.1.7 State Government Role 5-5
5.1.8 Financial Sustainability 5-5

6. Variations, Solutions, and Implementation Plans 6-1

6.1 Phases of Privacy and Security Solutions Project 6-1
6.1.1 Assessment of Variation 6-1
6.1.2 Analysis of Solutions 6-2
6.1.3 Implementation Planning 6-3
6.1.4 Factors Affecting Variations, Solutions, and Implementation Plans 6-3

6.2 Permission for Disclosure 6-4
6.2.1 Consent and Authorization Under the HIPAA Privacy Rule 6-4
6.2.2 Variation in Federal Law 6-7
6.2.3 Variation in State Law 6-8
6.2.4 Specially Protected Information 6-9
6.2.5 Variation in Internal Business Policies and Practices 6-11
6.2.6 Consumer Participation 6-12

6.3 HIPAA Privacy Rule 6-13
6.3.1 Flexibility in the HIPAA Privacy Rule and Interaction With State Law 6-13
6.3.2 Business Associate Agreements 6-15
6.3.3 Minimum Necessary 6-16
6.3.4 Covered Entities 6-17
6.3.5 Appropriate Disclosure and Redisclosure of Protected Health Information 6-19
6.3.6 Liability Concerns 6-21
6.3.7 Accounting of Disclosures 6-23

6.4 HIPAA Security Rule 6-23
6.4.1 Authentication, Authorization, Access Control, and Audit 6-25
6.4.2 Secure Transmission of Data 6-29

6.5 State Laws and Interstate Issues 6-31
6.5.1 General Issues in State Law 6-31
6.5.2 Public Health and Emergency Response 6-32
6.5.3 Medicaid 6-34
6.5.4 Licensing 6-35
6.5.5 Interstate Exchange 6-35

6.6 Trust in Security 6-36
6.6.1 Providers 6-37
6.6.2 Solutions and Implementation Plans 6-38
6.6.3 Consumer Trust 6-39
6.6.4 Solutions and Implementation Plans 6-39

6.6.5 Trust Within Other Stakeholder Groups....6-41

6.7 Standards for Patient Identification....6-41

6.7.1 Types of Patient Identification Used....6-42

6.7.2 Different Identification Systems: Common Challenges....6-42

6.7.3 Solutions and Implementation Plans....6-44

6.8 Cultural and Business Issues....6-45

6.8.1 EHR Adoption Issues....6-45

6.8.2 Business Practices and Terminology....6-46

7. Future Directions and Recommendations 7-1

7.1 Leadership and Coordination With Federal Initiatives....7-2

7.2 Incorporating Privacy and Security Policies and Practices Into Governance Models....7-2

7.3 Alignment of State and Federal Legal Environments....7-4

7.3.1 Aligning State Health Privacy Laws....7-5

7.3.2 Interpretation and Application of Federal Laws....7-6

7.4 Organizational Practice, Policy, and Guidance....7-8

7.5 Technology and Standards....7-9

7.6 Specially Protected Health Information....7-10

7.7 Adoption of Privacy Policies and Security Standards....7-11

7.8 National Privacy and Security Health Information Resource Center....7-12

7.9 Consumer Outreach, Engagement, and Education....7-13

7.9.1 Developing Processes for Involving Consumers and Consumer Groups in the Planning and Development of HIEs....7-14

7.9.2 Educational Materials Targeted to Consumers....7-15

7.9.3 Facilitating Involvement of Consumer Organizations....7-16

References R-1

Appendices

A State-level Activity Currently Being Planned or Conducted as a Result of Work on the Privacy and Security Project....A-1

B List of Stakeholder Groups....B-1

C Privacy and Security Health Information Exchange Scenarios Guide....C-1

D Nine Domains of Privacy and Security....D-1

E Schedule and Participation at Regional Meetings....E-1

F National Conference Agenda....F-1

G A Model for Assessing and Categorizing the Stage of Development of Health Information Technology and Health Information Exchange Across HISPC-Participating States G-1

H Glossary of Acronyms H-1

Figures

Number **Page**

3-1. Membership of Project Work Groups 3-4
3-2. Stakeholder Engagement Through Community Outreach 3-5
3-3. Membership of Variations, Solutions, and Implementation Planning Work Groups 3-6
3-4. Membership of Steering Committees and Legal Work Groups 3-7

5-1. Range of Current Electronic Health Information Activities Within States 5-3
5-2. Distribution of HISPC-Participating States by Stage of Statewide HIE Development 5-4

Tables

Number **Page**

2-1. Stakeholder Groups, by Membership of Work Groups and Participation 2-5
2-2. Consumer Membership on Work Groups and Participation through Outreach 2-7
2-3. Number of Consumers Engaged in Variation Assessment through Outreach..... 2-7

4-1. Purposes of Health Information Exchange 4-2

6-1. Purposes of Health Information Exchange and Relevant Scenarios 6-2
6-2. Benefits and Weaknesses of Approaches to Permission 6-6

EXECUTIVE SUMMARY

This report presents an overview of the work conducted by 33 states and Puerto Rico under the Privacy and Security Solutions for Interoperable Health Information Exchange contract funded and managed by the Agency for Healthcare Research and Quality (AHRQ) and the Office of the National Coordinator for Health Information Technology (ONC).

Scope and Purpose of the Nationwide Summary

The purpose of this Nationwide Summary report is to provide a comprehensive review of the work conducted by the state teams[1] throughout the course of this project. Although the primary sources of information described in the Nationwide Summary report are necessarily state-specific, the report affords the opportunity to look across the activities conducted by the 34 state teams and to better understand what policies and practices need to be in place within and across states to both protect health information and promote nationwide electronic health information exchange. This Nationwide Summary report is an effort to expand the ideas and plans the state teams have developed by identifying common challenges and areas for ongoing collaboration. The Nationwide Summary report also incorporates issues raised during discussions at the regional and national meetings and presents discussions of key issues, based on the expertise of the members of RTI's Technical Advisory Panel (TAP) regarding the often complex interactions between state and federal law. This report addresses the broader implications of the project, makes recommendations for federal action that can facilitate nationwide electronic health information exchange, and may serve as a roadmap for state and federal agencies establishing privacy and security policies governing nationwide electronic health information exchange.

The work represented in this report was conducted by project teams in the 33 states and Puerto Rico, which form the Health Information Security and Privacy Collaboration (HISPC) project. Although the landscape for privacy and security in the remaining states and territories likely has some unique characteristics, most of the issues discussed in this report cut across the entire nation.

Overview of the Privacy and Security Contract

In June 2005, the US Department of Health and Human Services (HHS) published the *Summary of Nationwide Health Information Network Request for Information Responses,* which contained responses from 512 organizations and individuals. In this report, privacy and security considerations were crosscutting, and nearly every response cited the importance of "patient privacy and reiterated that the American public must feel confident

[1] Throughout this report the 33 states and 1 territory are referred to as the *state project teams* or as the *state teams.*

that their health information is secure, protected, portable, and under their control" (p. 21). The report also noted major concerns among respondents about the varying applications and interpretations of the HIPAA Privacy and Security Rules being implemented by organizations and the challenges this variation would pose to nationwide electronic health information exchange. Respondents noted that the HIPAA Privacy and Security Rules allow for 2 hospitals to develop 2 different business practices, both compliant, for protecting privacy and security of health care records, and that this variation must be addressed if interoperable electronic health information exchange is to be achieved nationwide. Furthermore, the respondents noted that complications would occur both within and across states because of inconsistencies and differences between state privacy laws and federal laws.

The purpose of this Privacy and Security Solutions for Interoperable Health Information Exchange project has been to assess variations in organization-level business practices, policies, and state laws that affect electronic health information exchange and to identify and propose practical ways to reduce the variation to those "good" practices that will permit interoperability while preserving the necessary privacy and security requirements set by the local community.

Formation of the HISPC

The Health Information Security and Privacy Collaboration (HISPC) comprises 33 states and one territory, Puerto Rico. There is only one subcontracted organization per state, and each subcontracted entity was designated by the governor. Each state and territory 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. Each state or territory was expected to reach out to a broad range of stakeholders to include at a minimum:

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

Methodology

The methodology developed for the project was based on 3 key assumptions. The first assumption is that, in order for stakeholders to trust electronic health information exchange, decisions about how to protect the privacy and security of health information should be made at the local community level. Second, to accomplish this goal, discussions must take place to develop an understanding of the current landscape and the variation that exists between organizations within each state and, ultimately, across states. Finally, stakeholders at the state and community levels, including patients and consumers, must be involved in identifying the current variation, understanding the rationale that underlies the current business practices, deciding what the privacy and security requirements are, and developing solutions to achieve broad-based acceptance.

State teams followed a modified community-based research model that provided flexibility to each team to organize its leadership, steering committee, and work groups in ways appropriate to the needs of their current industry organization and market structure. Project teams followed a core methodology that framed discussions for the exchange of specific types of health information within 9 domains of privacy and security by using 18 scenarios as the starting point for work group discussions.

The 9 Domains of Privacy and Security

- User and Entity Authentication
- Authorization and Access Control
- Patient and Provider Identification
- Transmission Security
- Information Protection
- Information Audits
- Administrative and Physical Safeguards
- State Law
- Use and Disclosure Policy

All state teams were required to form a steering committee composed of state leaders and public and private stakeholders to provide leadership throughout the process and to sustain the effort beyond the end of the contract. Steering committee membership varied in accordance with the unique landscape and environment of each state and territory, but all committees were asked to include one member that represented the governor's office—either a senior policy advisor, cabinet member, or, in the case of one state, the lieutenant governor. The other members of the committees include high-level health care officials, such as directors of health insurance companies, health care, hospitals, and public health care systems.

Table ES-1 provides the number of stakeholders engaged during the assessment of variation process as reported by all 34 state teams. This table gives an idea of the scope of stakeholder input that has been incorporated into this work.

The general approach to the work consisted of 4 interrelated steps to conduct the Assessment of Variation. First, the Variations Working Group (VWG) members reviewed the 18 health information exchange (HIE) scenarios and generated a core set of business practices and policies consistent with the stakeholder roles represented in the scenarios. Project teams were then asked to categorize business practices as potential barriers to

Table ES-1. Number of Stakeholders Engaged in Assessment of Variations Process (All States Combined)

	Stakeholders Engaged in Variations Assessment through Community Outreach (Raw Numbers)	
Stakeholder Group	**(N)**	**(Avg.)**
Providers	1,630	48
Hospitals/health systems	341	10
Clinicians	240	7
Physicians and physicians groups	220	6
Community clinics and health centers	185	5
Professional associations and societies	157	5
Pharmacies/pharmacy benefit managers	85	3
Mental health and behavioral health	82	2
Long-term care facilities and nursing homes	74	2
Safety net providers	61	2
Homecare and hospice	44	1
Laboratories	43	1
Emergency medicine	42	1
Federal health facilities	37	1
Other health care providers	19	1
Technology and Health Information Experts	582	17
Privacy and security experts/compliance officers	141	4
Electronic health records experts	94	3
Health IT consultants	84	2
Quality improvement organizations	67	2
Technology organizations/vendors	58	2
Health information management organizations	56	2
Regional health information organizations	47	1
Other health data and technology experts	35	1
Consumers	458	13
Individual consumers	318	9
Consumer organizations and advocates	140	4
Other Government	243	7
Medicaid/other state government	193	6
County government	50	1
Public Health Agencies or Departments	213	6
Employers	198	6
Legal Counsel/Attorneys	181	5
Medical and Public Health Schools/Research	140	4
Payers	122	4
Law Enforcement and Correctional Facilities	37	1
Foundations/Other Policy Consultants	4	<1
Other	3	<1
Total	3,811	112

electronic health information exchange (eg, requirement for wet signatures); as potential enablers of or aids to electronic health information exchange; or as having no impact on the flow of information, whether on paper or electronically.

Second, the core set of business practices generated by the VWG was circulated to a broader group of stakeholders for validation and to generate additional business practices based on their experience. This step served to involve the broader stakeholder community, build consensus, fill gaps in the VWG membership, and check the accuracy of the practices generated by the VWG.

In the third step, the VWG reviewed the full set of collected business practices to ensure that the data were complete and sufficiently detailed for evaluation by the Legal Work Group (LWG); in addition, the VWG identified the policy driving the practice to better understand the rationale behind the practice(s).

Finally, the business practices that were flagged by the VWG were reviewed by the LWG to identify the legal drivers that might be relevant to better understanding the rationale behind the practice(s).

Current Nationwide Landscape for Privacy and Security Solutions

Analysis of the activity reported by the state teams reveals an emerging pattern that reflects the roadmap from paper-based health information exchange to full electronic health information exchange at the state level. The variation in the level of analysis, identification of solutions, and the scope and content of the implementation plans is driven by the current placement of the state on the road to statewide electronic health information exchange. One of the determining factors in the identification and selection of these priority solutions and implementation plans across states was the stage of development, adoption, and implementation of health information technology (HIT) and HIE initiatives within the state.

All state teams have some type of HIT/HIE activity currently under way, and these activities range from independent, isolated HIT efforts conducted by one health care organization (single organizations), to the implementation of one or more local or regional multiorganizational HIE efforts, to the early planning of a statewide electronic health information exchange effort, to the establishment of foundational components of a statewide initiative, to early implementation of a statewide HIE effort, to more mature, operating statewide implementations.

With respect to local or regional electronic health information exchange activity, all teams identified 1 or more such efforts currently under way within their states. Most of these efforts are set in defined geographic areas in the state, are funded through local, state, private, or federal funding, and involve 2 or more provider organizations. Some states have done extensive inventorying of both HIT projects and interorganization HIE initiatives. Ten

of the 34 state teams are currently considered to be in the early planning stages of statewide electronic health information exchange development. This stage includes states that have not yet identified or established an organization to facilitate the statewide planning process but do have an agency or government body conducting preliminary assessment of HIT/HIE efforts in the state. This stage also includes states that have an identified government body or entity responsible for developing a statewide plan. States in this group included Arkansas, Illinois, Iowa, Kansas, Mississippi, New Hampshire, New Jersey, Oklahoma, Oregon, and Puerto Rico.

Fifteen state teams have established some foundational components necessary for statewide electronic health information exchange development. These include states that have (1) identified and established a central body to coordinate HIE development; (2) appointed a governing body (board of directors); (3) established operating committees; and (4) completed a strategic plan or roadmap. States in this group included Alaska, Colorado, Connecticut, Kentucky, Louisiana, Michigan, Minnesota, New York, North Carolina, Ohio, Vermont, Washington, West Virginia, Wisconsin, and Wyoming.

Seven states were classified as having established early implementation, including Arizona, California, Florida, Maine, Massachusetts, New Mexico, and Rhode Island. In addition to the element identified in the previous stage of development, here the distinguishing factors were as follows: (1) some of the key roadmap implementation steps have been undertaken, (2) the statewide HIE initiative has selected a technology vendor, and (3) the state has begun implementing HIE pilots. In all cases in this group, the central coordinating body was a nonprofit entity.

This group was characterized by a fully functioning statewide HIE effort, albeit the effort may be supporting only 1 or just a few types of clinical electronic health information exchange (ie, clinical labs, medications, note documentation, billing, claims scrubbing). Only 2 states, Indiana and Utah, were considered to be at this stage of development.

Across the board, state government roles in the planning and implementation of statewide HIEs varied from active participation to being a co-lead facilitator, to serving as the lead convener and providing initial funding support for the planning process and, in some cases, funding the initial infrastructure investment needed to launch statewide HIEs.

For most states at a foundational level or early statewide implementation stage that have completed a statewide implementation plan, the financial plan called for a significant foundational support from state government, federal government, or both to launch the effort.

Assessment of Variation, Analysis of Solutions, and Implementation Planning

Section 6 in this report presents issues that state teams identified as critical and in need of resolution. First among those issues is the need to harmonize the approach to patient permission for disclosure.[2] Thirty of the 34 state project teams cited the need and process for obtaining patient permission to use and disclose personal health information as key to private and secure electronic health information exchange, and the area that requires the most work. Broad variation exists among organizational policies that determine when patient *consent* is required, how the *consent* is obtained and documented, and how patient permission is communicated to health care organizations, payers, and other outside entities. State teams suggested a wide range of solutions to address the differing definitions and applications of patient permission. One of the most frequently cited solutions was the creation of a common or uniform permission form for both paper and electronic environments. State teams proposed 3 general designs for permission documents: a uniform permission form used by all; a standardized permission form that includes certain elements, but may be modified based on institutional preferences; and models that would allow institutions to draft their own forms. Each option has positive and negative aspects, including the amount of work required to achieve consensus on the necessary elements and the complexity of managing those elements in an electronic system. Many state teams have indicated that they want to maintain the requirement for patient permission but make it more workable in an electronic environment, and they plan to fully catalogue state permission requirements (at least for treatment) and work to harmonize the permission process requirements.

Whatever solution the state teams identify must also accommodate federal laws that impose additional requirements on the exchange of certain types of health care information requiring patient permission for disclosure. The Family Education Rights and Privacy Act (FERPA) governs most school records; under FERPA's privacy and security regulations, information contained in a school health record is considered an education record (not *protected health information,* as HIPAA stipulates), which requires permission for disclosure, with the exception of health and safety emergencies (45 C.F.R. § 160.103; 34 C.F.R. § 99.31). The Clinical Laboratory Improvement Amendments (CLIA) were also cited for conflicts imposed on states because of ambiguous terms.

[2] The terms *consent* and *authorization* have specific meaning under various federal and state laws. For the purposes of this discussion we have adopted the neutral term *permission* to refer to the concept of obtaining written approval from a patient to use or release health information. The terms *consent* and *authorization* are used where appropriate (ie, in discussions of HIPAA's treatment, payment, and health care operations exceptions).

States also reported the need to incorporate requirements of federal laws governing the confidentiality of alcohol and drug abuse patient records and Medicaid information.[3] These topics are more fully discussed in Sections 6.2.4 and 6.5.

The state teams have made it clear that the interplay among the HIPAA Privacy and Security Rules, other federal laws that protect sensitive data, and state privacy laws creates a complex environment where what is required is not always clear. Some state teams have called for treating all health information as specially protected, which would raise the privacy bar but reduce the variation.

States reported many business practice variations based on different interpretations and applications of the requirements of the HIPAA Privacy Rule. Section 6.2 summarizes some examples from the state teams regarding HIPAA Privacy Rule issues that pose challenges to electronic health information exchange. State teams recommended 4 general categories of solutions to address the variation caused by differing applications of the Privacy Rule and state law: education programs; standard policies and practices; creation of a compendium of state law, federal law, case law, and preemption analysis; and requests for federal guidance. The acronym "HIPAA" has become a generic term for privacy and security practices, even though restrictions are often imposed by state law or practices resulting from misinterpretations of the HIPAA requirements. State teams planned to offer additional education for providers, perhaps as a continuing education requirement. The recommendation for education programs included suggestions for a variety of topics: addressing differences in state law and the HIPAA Privacy and Security Rules that pose challenges to electronic health information exchange; public misconceptions of the HIPAA Rules; specific areas of misunderstanding, such as use and disclosure of information to personal representatives; and definitions of terms as they apply to paper and electronic environments.

Standard policies and practices are another potential solution. State teams suggested creating policies that address routine exchanges of information both in regular and emergency circumstances. These exchange models would comply with both the HIPAA Privacy and Security Rules and state law. The policies and practices would have to be developed by the appropriate leadership body and be reviewed by a variety of stakeholders. Once developed, the body would disseminate the policies and offer educational programs to explain their significance and implementation strategy. This solution may prove useful in certain circumstances, but may be less feasible, given the wide range of circumstances and situations that organizations face. Alternatively, state teams suggested compiling relevant state law, federal law, case law, and preemption analyses. State privacy laws were generally passed over time and are frequently scattered throughout many chapters of the

[3] 42 C.F.R. pt. 2 uses the term *alcohol and drug abuse*. Most of the states used the term *substance abuse*. This summary has adopted the terminology from the federal regulation for consistency.

state code. Case law may also contain conflicting interpretations. State teams requested that the HHS Office for Civil Rights (OCR) publish de-identified case studies that describe the type of privacy lapses that are identified during enforcement activities and what corrective action was taken. It is important to note here that OCR now publishes specific but de-identified case examples of corrective action obtained from *covered entities* through enforcement of the Privacy Rule. Section 6.4 of this report discusses the variation in the interpretation and implementation of the HIPAA Security Rule, with state teams indicating that the majority of stakeholders were not familiar with appropriate security policies, procedures, and technical solutions. State teams found that legal standards for security are lacking at the state level and are generally perceived to be inadequate or vague. Sharing personal health information among institutions requires a significant degree of trust in the technology, and in the other organizations' ability to implement it. State teams found that much of the concern about security came from providers who were worried that entities receiving their data might not have security measures as robust as those of their own organization, and that they might be considered liable in case of a security breach. Related to this concern was a lack of understanding that security in health care is far more complex than just the adoption of appropriate technical standards. Thirty-one state teams offered technology-based solutions to security issues. The level of specificity in the solutions varied widely, from general statements that certain technical issues must be resolved to achieve an acceptable level of security to very specific and detailed discussions of how to resolve specific issues. For example, one report provided specific technology-based solutions to security issues encountered during the creation of an HIE program in their state, including user/entity authentication, access controls, patient and provider identification, protection of sensitive health information, protocols for information transmission, audits, and use and disclosure policies.

Specific state law and interstate issues are discussed in Section 6.5. The major source of variation in business practices and policies stems from each state's unique privacy and security laws. Some of these issues have roots in federal legislation, although the true source of variation often lies in the state statutes. A major reported source of variation, state law that applies to sensitive health information, is discussed in Section 6.2.4, which addresses the variation in permission requirements. Many of the proposed changes to state law are very specific and apply to a narrow range of circumstances in a single state. For example, one state has a burdensome law that requires extensive documentation of disclosures of information, even verbal communications, between medical staff treating a patient in a single facility. Identifying laws that create challenges to interoperability, understanding the reason that the law was passed in the first place, and determining potential solutions require a thorough legal analysis. State teams have carefully considered the implications of amending state laws and, in many instances, have created options for language that could be used to amend the relevant law, and have discussed the pros and cons of each choice, as well as the implications of leaving the law as is. These very specific

changes are not addressed in detail here, but the following are general areas in which state teams plan to amend state law:

- Update or create legal definitions of terms (ie, *medical record* or *record locator service*) to apply to electronic exchange.
- Amend state privacy laws that do not sensibly apply to electronic exchange to include protections for electronic data.
- Create enforcement mechanisms for any new privacy or security laws.
- Consolidate state law or compile a compendium of relevant state law, federal law, and case law to facilitate legal analyses.

State teams were careful to note that they wished to proceed cautiously in amending state law, observing that the change could have unintended consequences, such as inadvertently limiting exchange instead of facilitating it.

Trust continues to be a critical issue that affects the potential adoption and viability of electronic health information exchange. Section 6.6 discusses the concerns that consumers and providers expressed; it also outlines areas where underlying trust issues lead organizations to draft extremely conservative policies that contribute to the variation in business practice and policy. Consumer concerns focused on privacy risks arising from the implementation of new technologies and the potential for unauthorized disclosures of *specially protected health information* to payers and employers. Providers were principally concerned about potential liabilities arising from the activities of other participants in health information exchange and about consumers' lawsuits for inappropriate disclosures of their information; they were secondarily concerned about potential uses of patient information by payers, law enforcement, and public health officials. The latter concern had less to do with trust in the security of the EHRs themselves, and more to do with how these systems might manage the competing interests between groups about access to EHR data.

Trust emerged as a major underlying issue. In some cases, trust (or lack of it) seems to have been a motivating reason for the variance in business practices. In a number of cases, stakeholder groups (other than consumers) articulated their impression that consumer lack of trust was a critical issue, but the concerns were neither supported nor denied by consumer input. Ten of the reports lacked information that either expressly, or by reasonable inference, raised trust as a critical issue.

The ability to accurately identify patients across systems was an issue in many states: 16 state teams suggested technical solutions to this issue. For the most part, these state teams agreed that some system of identifying patients between entities must exist for true interoperability to occur, and that these systems must include stringent matching criteria to ensure that patient records remain confidential. A discussion of the importance of patient and provider identity matching is provided in Section 6.7. Many state teams reported other major challenges: the variability in methods across organizations to link patients to records,

and the lack of agreed-upon patient-to-record matching standards to apply when interorganizational electronic health information exchange is conducted. These challenges were not the case in uniquely identifying *providers* across the health care system, because new federal HIPAA regulations have now established a national standard unique identifier for health care providers (the National Provider Identifier [NPI]). Providers, payers, and others are required to fully implement the NPI by May 23, 2007.

Given the lack of a national (or state) unique patient identifier, state teams discussed several alternatives for future use under organized regional networks, and aimed at addressing the need for matching patients to their records across systems. One frequently cited mechanism was the record locator service (RLS), a centrally administered function of a health information network that provides the requester of data with the location of data about a specific patient. The RLS uses various identifying characteristics of individuals to create a match and to identify the location of health information for that individual.

State teams referenced a number of cultural and business issues that pose challenges to electronic health information exchange; these issues are discussed in Section 6.8. One example is concern about liability for incidental or inappropriate disclosures, which causes many stakeholder organizations to take a conservative approach to developing practice and policy. This concern is discussed in greater detail in Section 6.3.6. General resistance to change is another business issue that organizations face whenever a change occurs in how business is conducted, which in turn, can cause workflow modifications. Some individuals within organizations are comfortable with existing paper-based or manual systems and data exchange practices and processes, and they believe that current manual practices produce accurate data and are timely and effective. Implicit in some discussions is an assumption that security slows down the process: the data are secure but are not transmitted as fast as they can be with a quick phone call. In fact, most data exchanges take place via person-to-person contact, especially in emergency situations, and human judgment plays a large role in how and when information is exchanged. It will be critical to include these points at which human judgment is required in the specifications for any system developed to exchange information.

Recommendations for Future Directions

The goals for this project have been achieved. State teams assessed variation, developed solutions, and considered how to implement those solutions. Each team developed a body of knowledge that has been shared with stakeholders within each state, and many state teams have begun to move forward with their plans. Of necessity, each team worked within its own state environment in this first phase of the process; however, to reduce variation in practice, policy, and law to a manageable range for nationwide electronic health information exchange, state teams will need to work with one another and with existing federal initiatives. To reduce variation moving forward, a coordinated effort will be required so the

34 state teams can work with teams from the remaining 22 states and territories to resolve key issues and to ensure agreement on a manageable range of solutions that can be translated into the privacy and security requirements for nationwide health information exchange. State teams have prioritized their plans, based on the needs dictated by their unique local environment for electronic health information exchange. It will be important to cluster the state teams into collaborative work groups that will each work on a topic that is both a priority for each state or territory, but is also applicable to the other states and territories. Periodically, the collaborative work groups should come together to share their progress and get input from the broader nationwide collaborative.

The next goal is for the work of the collaborative work groups to be adopted nationwide. This model provides the central coordination necessary to ensure that the work reduces variation nationwide by allowing the stakeholders within each state to push the issues and recommendations up to the collaborative work group. The model also provides a mechanism for interaction with the appropriate federal initiatives. This process is naturally recursive, as new issues are raised and work groups evolve. In addition to the organization of the state teams moving forward in the short term, observations and recommendations based on the Nationwide Summary are provided in Section 7.

1. SCOPE AND PURPOSE OF THE NATIONWIDE SUMMARY

The purpose of this Nationwide Summary report is to provide a comprehensive review of the work conducted by the state teams throughout the course of this project. Although the primary sources of information described in the Nationwide Summary report are state-specific, the report affords the opportunity to review the activities conducted by the 34 state teams and to better understand what practices and policies need to be in place within and across states to both protect health information and promote electronic health information exchange nationwide.

State teams have identified practices, policies, and laws that are specific to their states and their unique health information exchange environments. Equally important, the state teams have established relationships among stakeholders, and they have catalyzed action within each of their states. A scan of the final state reports yielded a long list of activities and projects that are reported to be under way in many of the states either directly or indirectly as a result of the Privacy and Security Solutions project. In Appendix A, we present a table of activities that were reported by the state teams in the introductory sections of their final reports. Although this is not an exhaustive or comprehensive list of activities, it does provide an insight into future directions and some of the areas of work that the state teams have embarked on.

This Nationwide Summary report expands on the ideas and plans the state teams have developed by analyzing what they have done to identify common challenges and areas for ongoing collaboration. The Summary report also incorporates issues raised during discussions at the regional and national meetings, and presents authoritative treatments of key issues, based on the expertise of the members of the RTI Technical Advisory Panel (TAP) in areas such as those involving interactions between state and federal law.

Despite their differences, state teams have identified common challenges, and will need to meet common requirements to resolve them. Working together and sharing knowledge will enable states to harmonize solutions and align business practices to move toward nationwide health information exchange. This report addresses the broader implications of the project, makes recommendations for federal action that can facilitate nationwide health information exchange, and serves as a roadmap for federal agencies establishing policies governing nationwide health information exchange.

1.1 Description of the Scope and Purpose of this Report

This report is the final in a series of reports prepared under a contract entitled Privacy and Security Solutions for Interoperable Health Information Exchange, which was funded and managed by the Agency for Healthcare Research and Quality (AHRQ) and the Office of the National Coordinator for Health Information Technology (ONC). Under the terms of this contract, RTI International contracted with entities in 33 states and 1 territory to conduct an

assessment of variation in business practices related to health information exchange, identify practices, policies, and laws that might be perceived as barriers to electronic exchange of health information, suggest possible solutions to these barriers, and prepare plans to implement these solutions. As background, this report provides an overview of the contract goals, a review of how the Health Information Security and Privacy Collaboration (HISPC) was formed, and a summary of the methodology the state teams followed to conduct the assessments, develop solutions, and prepare for implementation.

Although many of the state teams have raised important issues, such as barriers to the adoption of health information technology (HIT) and business models for developing exchange organizations, this report focuses on the privacy and security issues described by the state teams. In addition, the completeness and limitations of the variations assessment process are analyzed to identify gaps and make recommendations for future work in this area. Issues are analyzed to identify those that should be considered for implementation through future project activities, including single-state solutions and clusters of solutions that lend themselves to teaming with other state teams. In addition, the completeness and limitations of the solutions analysis conducted by the state teams are reviewed to identify gaps and make recommendations for future solutions analysis. Similarly, the completeness and limitations of implementation planning conducted by the state teams are reviewed to identify gaps and make recommendations for future work in this area. Finally, the analysis provided by this report will inform other ongoing initiatives, such as the State e-Health Alliance, and includes recommendations for taking full advantage of the valuable work that has been completed.

1.2 Report Limitations

The work represented in this report was conducted by project teams in the 33 states and Puerto Rico, which form the Health Information Security and Privacy Collaboration (HISPC) project. Although the landscape for privacy and security in the remaining states and territories likely has some unique characteristics, most of the issues discussed in this report cut across the entire nation. The report does not include all aspects of each state's analysis and results. Privacy and security issues have many dimensions, and the report highlights only those considered the most significant or common across a number of states.

Finally, the report is limited by the extent to which it relies on state teams' existing knowledge and perceptions. State teams vary greatly in adoption, maturity, and experience with electronic health information exchange. For many states and many stakeholders, this project was the first substantive effort in this arena and, clearly, tremendous value will be gained by continued collaboration and sharing of ideas. Some state teams developed solutions and implementation plans based on limited knowledge of solutions developed or implemented elsewhere. State teams may have rejected a particular solution as infeasible, unaware that important groundwork had been completed in another region or state. This

report acknowledges this limitation and attempts to mitigate it by including authoritative treatments of key issues provided by expert members of the TAP. Further, common elements across state teams' reports are brought together and analyzed by topic area to provide additional perspective on how these issues are being addressed nationwide.

2. OVERVIEW OF THE PRIVACY AND SECURITY CONTRACT

Nationwide electronic health information exchange will represent a critical shift in the US health care system to improve quality by reducing medical error and health care costs. However, to accomplish this goal and to reap these benefits, the American public must accept and embrace nationwide electronic health information exchange. Consumers need to know that their information is appropriately protected. Much variation currently exists in the practices, policies, and laws that govern private and secure data exchange. To develop interoperable systems, some of this variation must be harmonized by adopting common policies so that organizations can meet consumers' needs for privacy, confidentiality, and security. At the same time, organizational business interests must be protected to minimize risk for the organization and develop trust between organizations.

2.1 Project Assumptions

Health information exchange (HIE) refers to the sharing of clinical and administrative data across the boundaries of health care institutions and other health data repositories. Health information exchange occurs daily, albeit much of it on paper, via fax, US mail, or phone. Electronic information sharing is called electronic health information exchange. Many stakeholder groups (payers, patients, providers, and others) realize that if data could be more readily shared, the safety, quality, and cost of health care processes would improve. From a cultural and technical standpoint, sharing health data is not easy. Stakeholders have competing priorities. Financial concerns, unresolved issues related to rights to access data, and privacy and security issues are among some of the hardest challenges to overcome.

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

Three basic assumptions underlie this effort:

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

2.2 Project Goals

The first goal of the Privacy and Security Solutions project was to identify variation in organization-level business privacy and security policies and practices, as well as state laws, that affect electronic health information exchange, and to discuss with stakeholders in each state the current protections and how those protections must be changed or updated as the organizations move from paper to electronic health information exchange. The second step was to document those practices that are protective and facilitate information exchange and incorporate them into proposed solutions. Next, after any barriers to electronic health information exchange were documented, the task was to identify the policy, legal driver, or other underlying rationale for the practice and to identify consensus-based solutions. The final step was to develop a plan to implement the solutions.

Two equally important goals were (1) to create sustainable collaborative networks of key stakeholders within states and communities to support future work and inform future electronic health information exchange activities and (2) to create a knowledge base that other states and communities could use as they address electronic health information exchange privacy and security issues.

2.3 Project Limitations

This project, which was conducted at the grassroots level following a community-based approach, necessarily required some tradeoffs to accomplish its goals. The analysts/researchers could have followed a rigorous scientific approach, developed a nationwide sample frame, selected a sampling of organizations within each state, conducted survey data collection, and drafted reports identifying problems in each state along with solutions and issues still needing resolution. However, the likelihood that these results would have been embraced and acted upon was in question. One decision made early in the process was that the work had to be conducted at the grassroots level, thereby engaging the stakeholders to review the issues and make the decisions, and then inform state and federal leaders about how they could help to make the initiative a success. Catalyzing the conversations among stakeholders was a critical component that could not be accomplished without engaging stakeholders in the process. With much more time, the design of the project could have perhaps incorporated both the community-based approach and scientific rigor. However, it is doubtful that the outcomes would have been different. To ensure that each state team engaged a broad range of stakeholders in the process and that the business practices identified by the state teams were comprehensive and represented the broad range of participating entities, RTI worked with the state teams to reach the necessary groups within their state. Many different stakeholder groups exist (and often many constituents exist within each stakeholder group), for example, the numerous types of health care providers. Seventeen groups were named in the request for proposals sent to

states and territories, with the option of identifying additional stakeholders (see Appendix B). Many additional constituents were identified as the work was completed.

The approach to conducting the work addressed representativeness in several ways. First, the assessment of variation was based on 18 scenarios developed to engage a wide range of stakeholders representing a wide array of purposes for health information exchange. Appendix C provides a complete set of the scenarios. Second, each participating state and territory was specifically required to demonstrate the capability to ensure participation by a range of stakeholders collectively representing the state's current environmental landscape, both within the stakeholder communities and geographically across each state. Third, the topic of representativeness was covered during the training of each state team to ensure that, as a practical matter, the appropriate groups would participate. Fourth, the design of the assessment process was recursive: practices identified by project teams were vetted with larger groups of stakeholders at several points in the assessment process to identify and fill gaps.

The ability to make scientific inferences based on statistical designs and sampling frames was not the intent of the contract. Instead, by following a feasible approach, Agency for Healthcare Research and Quality (AHRQ) and Office of the National Coordinator for Health Information Technology (ONC) enabled state teams to identify the most significant health information exchange privacy and security issues, on an aggressive timeline, in a rapidly changing environment, despite numerous differences among states in the level of adoption of systems to support electronic health information exchange, and despite many differences in the legal and business practice environments that could impede, facilitate, or remain neutral toward health information exchange.

Many state teams reported the constraint of the aggressive schedule as a limitation on the depth of their analysis and stated that they would clearly need to continue work to operationalize the solutions and plan for implementation. Specific constraints included difficulties in scheduling meetings with busy stakeholders and overcoming project learning curves for stakeholders. The need to educate stakeholders before they could become productive members of the work groups was particularly acute for the consumer groups.

One additional limitation of the aggressive schedule was that the state teams, especially those in the early stages of planning for widespread electronic health information exchange, had limited time for collaboration outside of their state team. This need to collaborate was highlighted at the 10 regional meetings and at the national meeting. Finally, a number of state teams felt constrained by the absence of a practical model showing how exchange might occur within their states and where in the process safeguards might be put into place.

2.4 Limitations of Stakeholder Group Participation

State teams assembled knowledgeable steering committees and work groups, and engaged stakeholders from the broader community, as required by the contract, to vet and evaluate the work of the teams and fill gaps on the teams. State teams reported stakeholder group representation as part of the final Assessment of Variation and Analysis of Solutions report. They reported the stakeholder groups represented by the membership of their steering committees and work groups, as well as those engaged through community outreach during variations assessment, solutions analysis, and implementation planning (see Table 2-1).

Each state team was provided a matrix showing 17 stakeholder groups, 18 health information exchange scenarios, and each stakeholder group's primary or secondary interest. Additional stakeholder group categories were developed as the project progressed, and state teams reported stakeholder participation in detail, often using terminology that expanded on the original list of stakeholder groups. Each team was asked to report the stakeholder groups represented by the members of their work groups and the stakeholder groups that were involved through outreach to the broader community. These reports used a template that included 30 categories (see Table 2-1). All state teams submitted a completed table as part of the final Assessment of Variation and Analysis of Solutions report. Summary tables based on the information supplied by the state teams are presented and discussed in detail in Section 3.

Consumer engagement, in particular, warranted further discussion. The aim of the project was to identify and develop solutions to facilitate electronic health information exchange while preserving consumer privacy and security protections. Thus, the meaningful participation of consumers/consumer groups as key stakeholders was essential, but whether it was sufficient to ensure consumer acceptance of electronic health information exchange is still open to debate. Consumer fears of inappropriate use and disclosure could impede attempts to move toward nationwide electronic health information exchange, regardless of the level of consumer involvement achieved by the state teams.

Most state teams were able to engage consumers (see Table 2-2). Consumers were included as members by at least 65% of all project steering committees and work groups, excluding Legal Work Groups (LWGs). Consumers were engaged by over three fourths of state teams during variation assessment and by over two thirds of all state teams during solutions analysis and implementation planning.

Over 450 individuals classified as consumers were engaged by state teams during variation assessment. One hundred forty of these individuals were consumer advocates or represented consumer organizations (see Table 2-3). Additionally, state teams recognized that all project participants were consumers, in that they had an interest in the privacy and security of their own health information, as well as having access to the highest quality care at the lowest cost. A few state teams reported these participants as their consumer

Table 2-1. Stakeholder Groups, by Membership of Work Groups and Participation

Stakeholder Group	Membership of Work Groups					Participation Through Outreach		
	Steering Committee	Variations Work Group	Legal Work Group	Solutions Work Group	Implementation Planning Work Group	During Variations Assessment	During Solutions Analysis	During Implementation Planning
Technology and Health Information Experts	**33**	**33**	**30**	**33**	**33**	**29**	**29**	**29**
Privacy and security experts/compliance officers	13	24	21	28	25	26	22	22
HIT consultants	17	22	14	25	27	24	23	22
Electronic health records experts	14	22	8	21	17	22	19	16
Quality improvement organizations	18	21	10	17	16	22	20	20
Regional health information organizations	13	17	12	15	17	17	17	16
Health information management organizations	9	16	8	17	14	16	14	14
Technology organizations/vendors	8	11	6	19	19	17	15	14
Other health data and technology experts[a]	5	6	2	5	5	6	4	4
Providers	**33**	**32**	**31**	**32**	**31**	**32**	**30**	**29**
Hospitals/health systems	28	32	27	31	30	29	28	28
Physicians and physicians groups	28	30	14	28	26	31	30	26
Professional associations and societies	23	27	21	23	22	25	22	19
Clinicians	22	29	10	27	20	28	27	22
Community clinics and health centers	15	27	10	20	18	27	15	15
Mental health and behavioral health	13	20	8	18	12	23	18	14
Pharmacies/pharmacy benefit managers	13	24	4	15	9	29	16	10
Long-term care facilities and nursing homes	8	21	4	10	8	24	14	9
Federal health facilities	10	16	2	8	8	15	10	6
Homecare and hospice	7	17	3	9	8	22	11	10

(continued)

Table 2-1. Stakeholder Groups, by Membership of Work Groups and Participation (continued)

	Membership of Work Groups					Participation Through Outreach		
Stakeholder Group	Steering Committee	Variations Work Group	Legal Work Group	Solutions Work Group	Implementation Planning Work Group	During Variations Assessment	During Solutions Analysis	During Implementation Planning
Emergency medicine	4	16	4	11	8	22	13	11
Laboratories	4	15	6	9	7	20	8	6
Safety net providers	8	12	5	8	8	19	8	8
Other health care providers[b]	6	3	1	6	4	6	8	8
Legal Counsel/Attorneys	**25**	**22**	**34**	**31**	**30**	**26**	**25**	**25**
Public Health Agencies or Departments	**25**	**31**	**24**	**32**	**28**	**30**	**27**	**24**
Other Government	**31**	**29**	**23**	**26**	**24**	**28**	**25**	**25**
Medicaid/state government except public health	30	27	22	24	24	28	25	25
County government	4	11	4	6	7	13	5	7
Payers	**28**	**27**	**21**	**25**	**21**	**27**	**28**	**23**
Medical and Public Health Schools/ Research	**25**	**23**	**20**	**25**	**24**	**28**	**25**	**22**
Consumers	**22**	**22**	**17**	**26**	**25**	**26**	**23**	**24**
Consumer organizations and advocates	17	17	12	21	21	24	21	21
Individual consumers	12	16	7	19	17	20	14	16
Employers	**17**	**17**	**8**	**12**	**13**	**21**	**14**	**16**
Law Enforcement and Correctional Facilities	**0**	**15**	**1**	**7**	**4**	**19**	**7**	**8**
Other[c]	**1**	**3**	**4**	**5**	**5**	**2**	**2**	**3**
Foundations/Other Policymakers and Consultants	**2**	**3**	**0**	**1**	**1**	**2**	**1**	**1**

[a]Examples include "health information directors," "IT directors," "technology expert," "wireless communication services," "communications," and "transcription service."

[b]Examples include "radiology," "dental," "chiropractic," "osteopathic," and "nursing."

[c]Examples include "state law reform specialist," "National Conference of Commissioners on Uniform State Laws (NCCUSL)," "medical ethicist," "school health," and "regional representation."

Table 2-2. Consumer Membership on Work Groups and Participation through Outreach

HISPC Work Group/Project Phase	State Teams Reporting Consumer Membership/Participation (N = 34)	(%)
Steering Committee	22	(65)
Variations Work Group	22	(65)
Legal Work Group	17	(50)
Solutions Work Group	26	(76)
Implementation Planning Work Group	25	(74)
Outreach during Variations Assessment	26	(76)
Outreach during Solutions Analysis	23	(68)
Outreach during Implementation Planning	24	(71)

Table 2-3. Number of Consumers Engaged in Variation Assessment through Outreach

Stakeholder Group	Number of Stakeholders Engaged in Variations Assessment through Community Outreach
Consumers	**458**
Individual consumers	318
Consumer organizations and advocates	140

representatives, although they were unlikely to be representative of typical health care consumers.

Yet, even these participation figures reveal that members of this key stakeholder group were not engaged in every state in every stage of this project. In addition, several of the scenarios examined in this project addressed the exchange of health information related to health conditions generally considered to be particularly sensitive, such as mental health, substance abuse, HIV/AIDS, and genetic information. Some proposed solutions focus on changing the level of protection for this sensitive information. It is not possible, however, to determine the extent of participation of consumers/consumer groups representative of these sensitive health conditions from the information reported by the state teams.

The reasons for lack of full consumer participation were diverse. State teams attributed this variously to the complexity of the scenarios, consumers' lack of familiarity with Health Insurance Portability and Accountability Act (HIPAA) and the state legal and business practice environment, and the technical nature of security solutions. Educating consumers to enable them to participate effectively was time consuming and only partially successful. A few state teams reported encountering consumers who assumed that widespread electronic health information exchange already exists, based on the ease and frequency of information transmission in other sectors today.

Most state teams were keenly aware of the importance of consumer buy-in and made numerous recommendations for consumer education as part of implementation planning to ensure that consumers can make informed choices about when and how their health information is exchanged.

One challenge facing increased consumer acceptance of electronic health information exchange is that the risks of inappropriate disclosure and identity theft are highly visible, easy to understand, and personal. Achieving this level of consumer engagement does not mean that consumer acceptance or buy-in has necessarily been achieved in these states, although essential first steps have been taken. Consumers need to be presented with enough information about risks and benefits of electronic health information exchange to enable them to make good decisions about whether and how to participate. They need concrete, personal examples of the benefits of electronic health information exchange, eg, electronic registration so that patients do not have to repeatedly give the same information every time they see a doctor and the availability of their health information in times of emergency. They need easy-to-understand information about their privacy rights and the security of health information systems. And they need to know what action will be taken against people or organizations that use or disclose their information improperly. Consumer engagement in the Privacy and Security Solutions project, whether through membership on work groups or through outreach, is only the first step in a challenging process.

3. FORMATION OF THE HEALTH INFORMATION SECURITY AND PRIVACY COLLABORATION

3.1 Procurement Process

Subcontract awards to the state teams were made through a competitive bidding process. In early January 2006, RTI released a Request for Proposals (RFP) that provided detailed information on the requirements for each state project, guidelines for submitting the proposal, and the type of support that would be provided by RTI and the National Governors Association (NGA). The RFP outlined the work that was to be completed by each entity submitting a proposal (offeror) within the 11-month contract, including an examination of privacy and security policies and business practices regarding electronic health information exchange, assembling and working closely with a wide range of stakeholders in the state, and developing an implementation plan to address organization-level business practices and state laws that affect privacy and security practices to permit interoperable health information exchange (HIE). Only one proposal per state was accepted, and each submission required inclusion of a letter from the governor's office designating the entity as the official offeror.

In total, 43 proposals were received on the due date of March 1, 2006. The technical proposals were separated from the cost proposals upon receipt, and only technical proposals were evaluated during the first phase. Each individual proposal underwent a thorough evaluation process by team members from RTI, the NGA, and the RTI Technical Advisory Panel (TAP). A single reviewer from each organization was provided a standard evaluation form, which assigned points to each specific section outlined in the RFP; points were awarded based on the strength of response to the expected criteria. Team members from RTI and the NGA held an all-day meeting to compare their evaluations and rank the candidates according to the reviewers' consensus. Once the proposals had been ranked according to technical merit, the cost proposals were evaluated to determine if they were sound and within the guidelines provided in the RFP.

RTI awarded subcontracts to as many states and territories as possible, by rank of technical merit, up to the funding limit allocated under the prime contract. A total of 34 subcontracts were awarded to the states and one territory to form the Health Information Security and Privacy Collaboration (HISPC).

3.2 Work Groups

All state teams were asked to form a series of workgroups to lead each major task. These work groups included a Variations Work Group (VWG), Solutions Work Group (SWG), Legal Work Group (LWG), and Implementation Plan Work Group (IPWG). Each work group had a specific mandate, although nearly all states made a conscious effort to ensure continuity

between the assessment stage and the solutions stage by including members of their VWG and LWG in their SWG and then adding key resources through targeted recruitment.

The VWG's primary task was to examine the business practices collected by the state project staff for variations in practice that indicated barriers to appropriate electronic health information exchange, and to identify best practices. They worked in parallel with the LWG, which was composed of lawyers and other HIPAA and health care compliance experts. Their task was to examine the legal and regulatory drivers behind the business practices.

The results of the analyses were then sent to a separate subset of stakeholders—the SWG—who assembled proposed solutions to the identified barriers to appropriate health information exchange. Many states noted that the composition and the direction of the SWG evolved through time, depending on the particular barriers and the knowledge and experience required to address them.

This work was then passed on to a fourth work group—the IPWG—that assembled achievable work plans to implement the proposed solutions identified by the SWG. A number of states also encouraged continuity in membership between the SWG and IPWG, with the guidance to include experts in health care policy from their state as well as additional consumers, if such representation was not already included.

3.3 Stakeholder Outreach

After the state teams identified their core team members, they began to identify stakeholders who were either interested in the project goals, who had health information technology (HIT) experience, or who added another perspective to the discussion of implementing a secure interoperable HIE system in the state. As expected, some states had an easier time with this process than others. For example, states that had explored this initiative prior to the Privacy and Security Solutions Project already had functional relationships with stakeholders in their states. Therefore, identifying stakeholders was less of a challenge for these state teams.

However, these states reported that participant burnout was a problem. Particularly in small states, teams had to recruit repeatedly from the same pool of stakeholders, and they feared rejection because these volunteers might not have time to commit to the project. Some states used a snowball or network sampling method that relied on existing sample members from a unique or hard-to-find population to nominate additional sample members. Some states addressed this problem by asking their stakeholders to identify someone else that could represent their perspective, if they were reluctant to participate. This tactic proved successful; usually the original stakeholder agreed to volunteer, or the team's stakeholder pool increased by the introduction of a new participant.

Some state teams found their outreach to stakeholders to be productive by first educating a larger group of stakeholders who had not been involved in electronic health information exchange initiatives about the Privacy and Security Solutions project. Again, they used the snowball recruiting strategy. If the person attending the informational presentation was not interested or available to participate in the project, he/she usually referred the team to another available person. Some teams reported that, through this process, they met new stakeholders they might have overlooked, and they have since made meaningful alliances and sound advances toward achieving private and secure health information exchange.

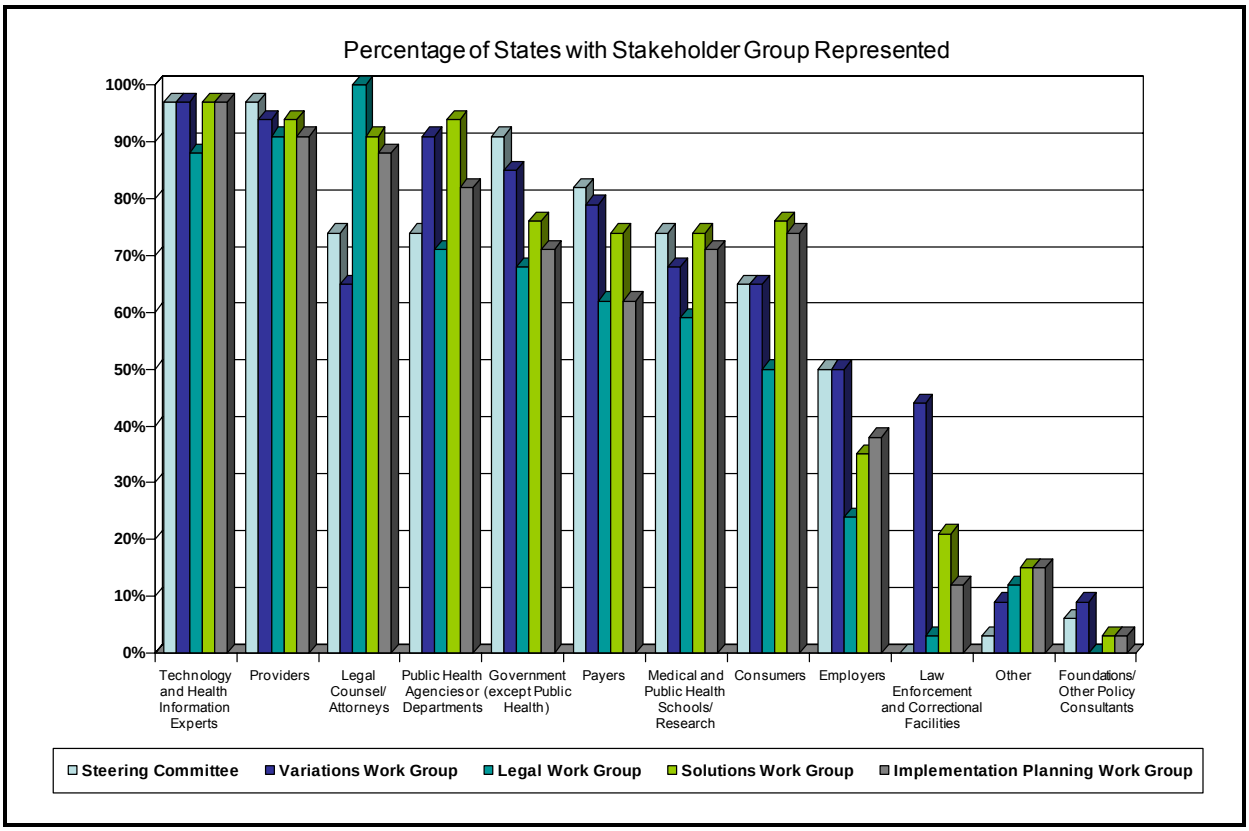
True to the project's design, stakeholders, once identified, were engaged in the different phases of the project via the work groups discussed in the previous section. In some instances, state teams reported that the same stakeholder(s) were involved throughout the project. Figure 3-1 shows the membership of the project work groups, and the percent of the states with stakeholder representation. Please note that the consumers label on this chart includes both individual consumers and consumer organizations.

The work groups matched the following stages of the Privacy and Security Solutions project:

- **Assess and analyze the impact of organization-level business policies and state laws.** In the first part of this task, stakeholder work groups identified business practices that impeded interoperability, and they determined whether a business or an information technology (IT) solution existed to remove the impediment. Next, the state teams worked with stakeholders to compare and contrast state laws and the HIPAA Privacy and Security Rules; categorize privacy and security laws in the state and the identified outliers; make the distinction between laws that are highly prescriptive and those permitting wide latitude; and map business policies and practices to the HIPAA Rules and other applicable federal and state privacy and security laws.
- **Identify solutions and develop an implementation plan.** State teams collaborated with stakeholders to review the practices identified as impediments or challenges and identified a range of business or IT solutions to be considered by a broader group of stakeholders within each state.
- **Develop implementation plan.** The culminating step was for the work groups to develop a responsive, actionable implementation plan that included careful consideration of risk, cost, and likelihood of success for the state. The plans included detailed timelines, important milestones, and cost estimates. The state teams also discussed the findings and rationale for the plan, as well as the strategy for developing public education and training materials.

The Agency for Healthcare Research and Quality (AHRQ) National Resource Center provided access to a private portal for state team communication. In addition, teams established various methods of maintaining open communication with the stakeholders throughout the project, including webinars, Wiki sites, state websites, e-mail, teleconferences, face-to-face meetings, ad hoc telephone calls, and targeted mailings. The goals for communication were to establish a trusting, respectful environment, identify the tools to allow an unencumbered exchange of information for the work groups, and support feedback to advance the project.

Figure 3-1. Membership of Project Work Groups

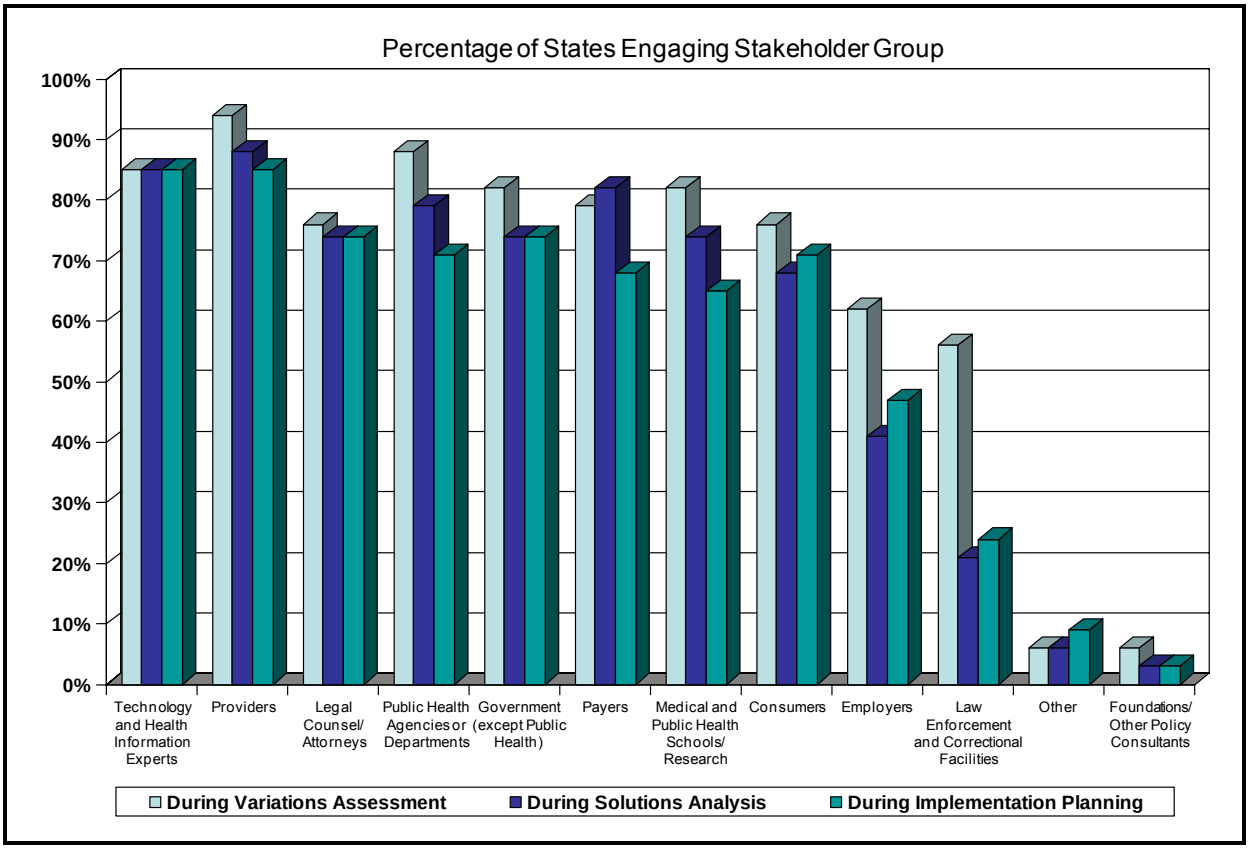


Note: "Consumers" on this chart include both individual consumers and consumer organizations.

State teams used a variety of collaborative mechanisms to develop a collaborative environment. For example, one state held an all-day retreat for all project work groups. A few state teams conducted combined work group sessions (ie, VWG and the LWG). A number of teams (8) held focus groups to learn more about the stakeholders' viewpoints. Three state teams conducted follow-up interviews with stakeholders who had little or no representation in the focus groups to make certain their perspectives were included. Another state team reported that the VWG established "study teams" with constituents to ensure that business practices were fully represented, and another state's LWG used the same model to identify legal issues.

Most states tried to be as inclusive as possible. For example, state teams sought to represent their state's geography by engaging stakeholders from rural, urban, suburban, large-populated, and small-populated areas. One state team believed that a series of news articles motivated additional stakeholders to call the Privacy and Security Solutions project director to voice their comments, concerns, and to provide additional business practices. All teams made an earnest effort to identify and provide outreach to as broad a stakeholder group as possible. Figures 3-2 and 3-3 provide a graphic representation of the stakeholders engaged by state teams during the various stages of the project, and their membership.

Figure 3-2. Stakeholder Engagement Through Community Outreach



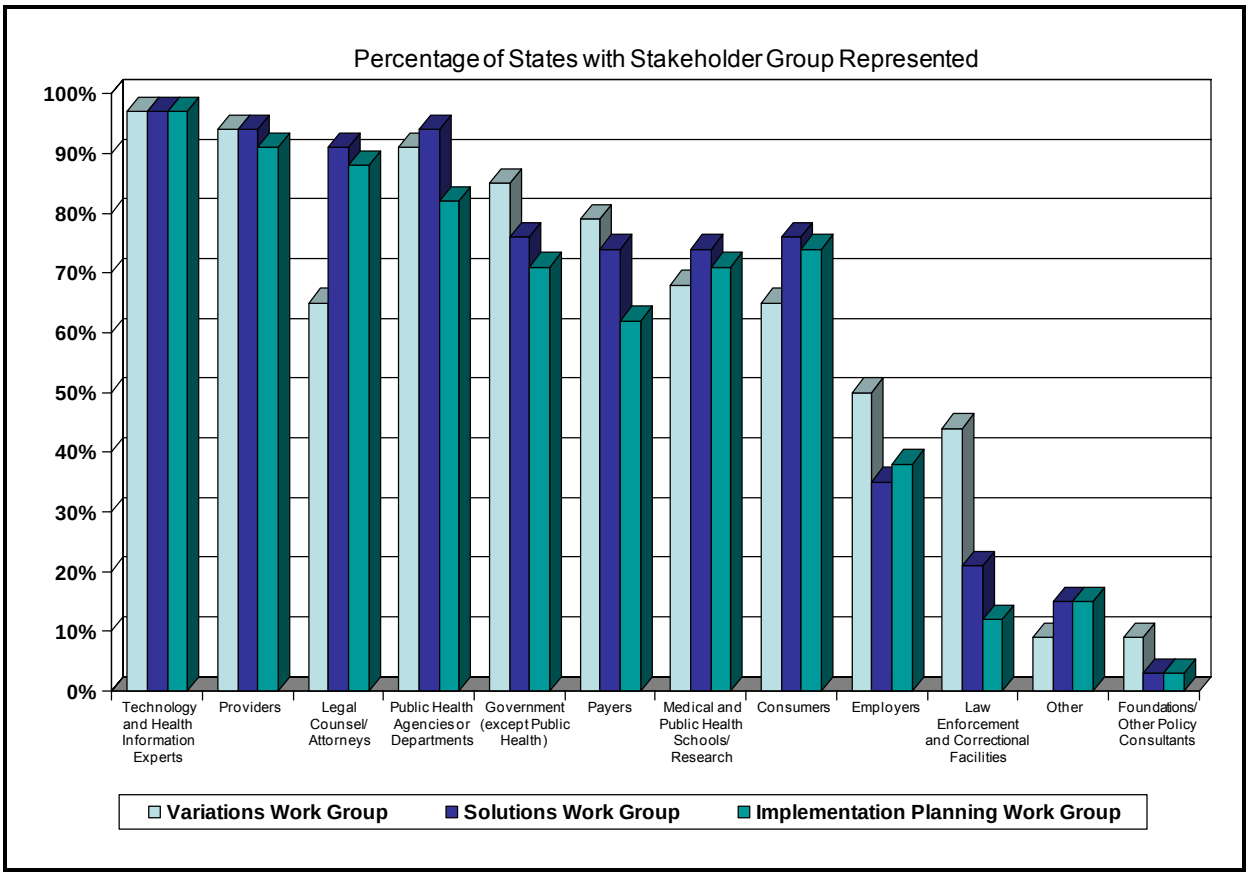
Note: "Consumers" on this chart include both individual consumers and consumer organizations.

3.4 Steering Committees

The steering committee was charged with providing strategic direction and general governance to state teams. Composition and size of the steering committee varied by state, as did the formation of the committee. One steering committee was composed of health care business executives, statewide health industry leaders, and a legal committee (public and private attorneys specializing in health care privacy and security law). Some governors appointed or designated the Privacy and Security Solutions project steering committee members. In other states, steering committee members were recruited from an established HIE stakeholder coalition because of the coalition's broad distribution and resource network, and their willingness to guide the project.

Common denominators across the state team steering committee members were the level of subject matter expertise and the commitment to the Privacy and Security Solutions project . Generally, the steering committee was a collaborative group of private and public health care and HIT industry stakeholders. In one state, the steering committee members also attended and participated in the VWG meetings as stakeholders.

Figure 3-3. Membership of Variations, Solutions, and Implementation Planning Work Groups



Note: "Consumers" on this chart include both individual consumers and consumer organizations.

Several states added an advisory board to the organization structure. In those states, the steering committee concurred that the advisory board and its subsequent committees were necessary to create an actionable work plan, to resolve outstanding issues, and to implement privacy and security solutions. The advisory group met more frequently than the steering committee, and the teams that used this model found it helpful, particularly in the beginning phase of the project when guidance and feedback were especially needed.

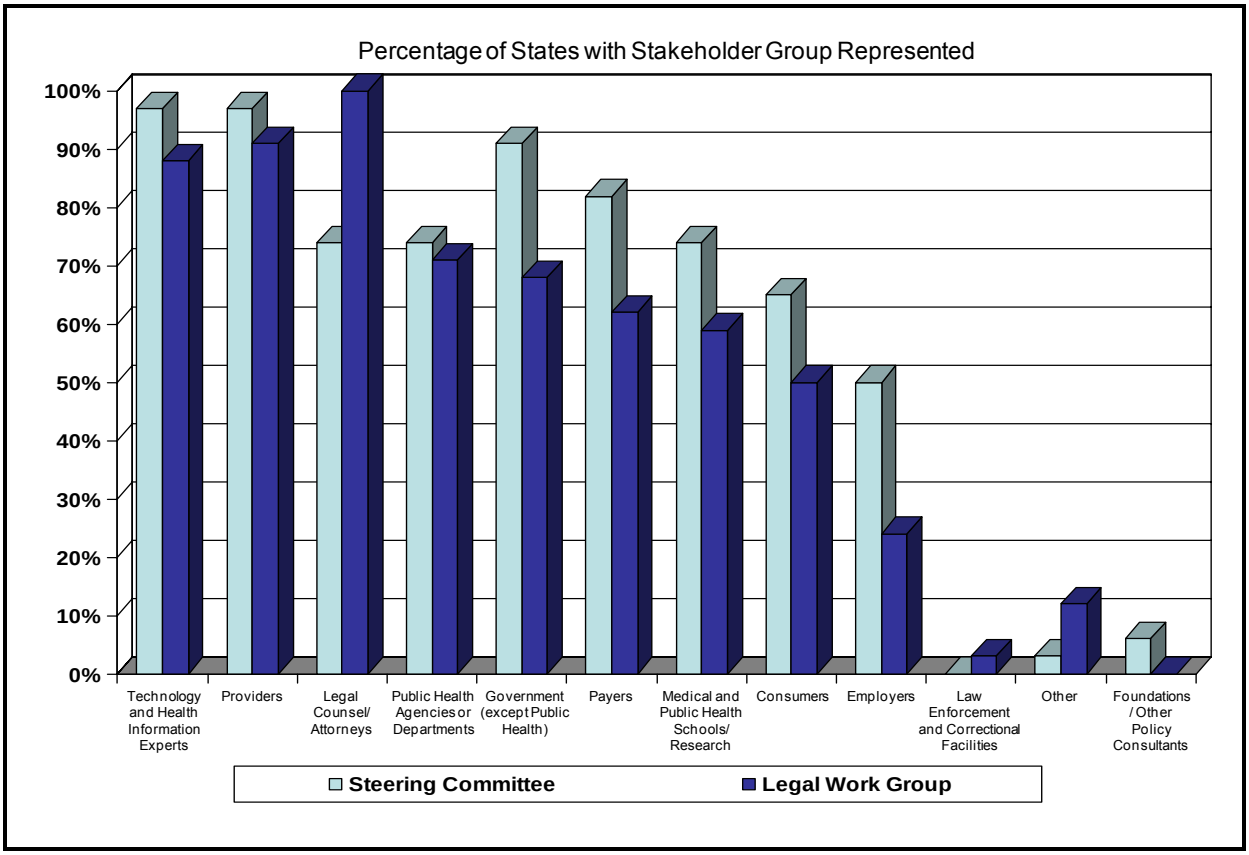
Many state teams also relied on the steering committee to assist in data collection efforts. A number of teams reported that potential members for each work group were identified through direct solicitation by the steering committee. Teams devised ways to maintain open communication with their steering committee. Some teams posted the reports on their private websites, while other teams utilized e-mail. One state reported that they posted highlights about the project on the websites, and also spotlighted the project in the state's bimonthly health care newsletter.

The steering committee provided guidance to the project management team and oversight in the development of all work products. One state reported that the steering committee

developed a methodology that allowed team members to draw on their natural strengths. According to the state's final reports, the steering committee's support, along with the expertise of the stakeholders, contributed to the development of beneficial work products to advance the goal of secure and private electronic health information exchange in the state. To that end, one governor's office is currently reviewing an executive order that would continue the role of the Privacy and Security steering committee as an interim step toward creating a proposed quasigovernmental organization.

Another state reported that, as the result of steering committee recommendations, the feasibility of successful implementation of privacy and security protections has been advanced by channeling the project's efforts through an ongoing demonstration project that is already funded and is soon to be implemented. This project's guidance has been shown to be precisely what was needed to galvanize community attention on the most important privacy and security issues for those who envision the proliferation of interoperable health information exchange in the state. Figure 3-4 displays the mix of subject matter expertise provided by members of the steering committee and LWGs, and the percent of states with stakeholder group representation.

Figure 3-4. Membership of Steering Committees and Legal Work Groups



Note: "Consumers" on this chart include both individual consumers and consumer organizations.

4. METHODOLOGY

This section describes the key components of the project's methodology, beginning with a discussion of the approach. The second section describes the methodological tools and support materials developed to facilitate the implementation of the design, including the training provided to the state project teams. The third section discuss the procedures states followed to identify organizational business practices, assess legal drivers, and develop solutions. The final section discusses a set of regional meetings and a nationwide conference that facilitated the collaborative process within and across states.

4.1 Approach

A modified Community-Based Participatory Model (CBPM) was developed for this project. The CBPM research model requires that the stakeholders have maximum involvement in the process using a standard set of tools and support for each state team to assure consistency in process and comparability of outcomes. Developing consensus-based solutions to privacy and security issues requires the full involvement of stakeholders to identify challenges, develop the solutions, and agree on feasible implementation plans.

Answering fundamental questions related to implementing a secure electronic health information exchange system called for the state teams to identify and assess the organizational-level business practices, policies, and laws associated with privacy and security. A detailed understanding of variations of business practices required exploring operations, management systems, and communication patterns. This requirement, coupled with a strong emphasis on engaging a broad base of stakeholders in the state activities, led to the framework of participatory action research. Creswell (2003) suggests the following summary (Kemmis and Wilkinson, 1998) of key features of the approach to understand this model of research.

1. Participatory action is recursive or dialectical and focuses on bringing about a change in practices. Thus, at the end of advocacy/participatory studies, researchers advance an action agenda for change.
2. It focuses on helping individuals free themselves from constraints in the media, in language, in work procedures, and in relationships of power in educational settings.
3. The aim of advocacy/participatory studies is to create a political debate and discussion so that change will occur.
4. It is practical and collaborative because it is an inquiry completed with others rather than on or to others. In this spirit, advocacy/participatory authors engage the participants as active collaborators in their inquiries.

The project was also designed to use the qualitative strategy of grounded theory as the variation in business practices was identified and vetted by the state teams. Creswell (2003) uses the description provided by Strauss and Corbin (1990, 1998) to explain the process.

Grounded theory involves using multiple stages of data collection and the refinement and interrelationship of categories of information. Two primary characteristics of this design are the constant comparison of data with emerging categories and sampling of different groups to maximize the similarities and the differences of information. Additionally, state teams used focus groups and one-on-one interviews to collect information on organization-level business practices, policies, and the legal rationale underlying each.

4.2 Methodological Tools and Support

Each state team was provided with computer-assisted tools and supporting materials to facilitate the assessment of variation, identification of solutions, legal evaluation, and implementation planning. Using a framework of 9 domains of privacy and security (see Appendix D for a more detailed description of the domains), a process was designed in which stakeholders in each state reviewed hypothetical scenarios to foster discussion in 11 areas that were typically the subject of state and federal law and regulations. These scenarios provided a common set of contexts for identifying organizational business practices and assured that a variety of type of health information exchanges was considered. Under a subcontract with RTI, the American Health Information Management Association (AHIMA) prepared 18 health care scenarios ranging across the 11 purposes for health information exchange listed in Table 4-1. (The scenarios are presented in Appendix C.)

The 9 Domains of Privacy and Security

- User and Entity Authentication
- Authorization and Access Control
- Patient and Provider Identification
- Transmission Security
- Information Protection
- Information Audits
- Administrative and Physical Safeguards
- State Law
- Use and Disclosure Policy

Table 4-1. Purposes of Health Information Exchange

Treatment	Health care operations/marketing
Payment	Bioterrorism
Regional health information organizations	Employee health
Research	Public health
Law enforcement	State government oversight
Prescription drug use/benefit	

RTI worked with the Agency for Healthcare Research and Quality (AHRQ) National Resource Center (NRC) to develop a web application and database that allowed project teams to capture and store business practices and link each practice to one or more of 9 privacy and security domains as well as to specific state privacy and security laws. The information collection process within each state (described below) was iterative to allow for broad-based

participation throughout the process to improve coverage. The NRC also provided web portal space to each team and the project as a whole to facilitate communication among the states and members of the project team. Information about the state teams and products of this work can be found at http://healthit.ahrq.gov.

The assessment tool (AT) was developed as a web-based data entry facility and a database for storing business practice data gathered from the set of common scenarios used in the assessment. On the website, user login and passwords protected unauthorized entry of information into the tool. During the assessment process, a free-standing version (that is, unconnected to the Internet) was used in settings where Internet access was impractical. Each state team provided at least one individual to serve as the content manager for the project team. The AT was integrated into the state team private workspace on the National Resource Center portal. Any individual with login access to the private workspace could view the AT data; however, only those with the appropriate level of permission could manipulate the data. The structure of the AT permitted each level of user to add on to what was previously created (including uploading data from the freestanding application). Specifically, once the business practices were added within the AT, members of the Variations Working Group (VWG) accessed those business practices to begin review and compilation, and the Legal Working Group (LWG) accessed those items to begin to identify legal barriers. The business practices could be accessed, sorted, and exported in various ways to facilitate reporting.

4.3 Process

Although the 34 state teams were required to follow this general framework and practices and other information in the provided application, they were also provided some latitude in how to organize project work groups and solicit information from stakeholders. The protocol was, basically, the assembly of stakeholders, then serial meetings of the VWG, LWG, Solutions Work Group (SWG), and Implementation Plan Work Group (IPWG). Upon completion of the meetings, the collected business practices were archived and loaded in the web portal for dissemination to the stakeholder community for review and comment and opportunity to add to the business practice roster. The assembled business practices were then transmitted to the LWG for analysis. The VWG was tasked to identify business practices related to the 18 scenarios and 9 domains provided by RTI.

The business practices were collected during a series of meetings of the participating stakeholders who were each asked to describe practices, policies, and processes for each scenario. The database provided fields for entering the following information about each practice:

- Business Practice Name,
- Business Practice Long Description,

- Scenario # (1-18),
- Classification (barrier, not a barrier, unassigned),
- Domain # (1-9),
- Policy Short Description,
- Policy Long Description,
- Stakeholder Entity,
- Legal Driver Description,
- Legal Driver Reference Number, and
- Cause (nonlegal drivers).

The VWG examined the business practices for variations that may have introduced barriers to health information exchange, and also to identify best practices. Working in parallel, the LWG examined the legal and regulatory drivers behind the business practices. The results of the analyses were then sent to the SWG who developed proposed solutions to the identified barriers. (A barrier was defined as a business policy or practice for which major legal or procedural changes must be developed and implemented if interoperability is to occur.) This work was then passed on to the IPWG, which assembled achievable work plans to implement the proposed solutions the SWG identified.

All state teams functioned within the principles RTI established at the outset of the project: to strive for inclusiveness and broad outreach to stakeholders; to protect the confidentiality of participants; to comply with project parameters required of all state subcontractors to ensure consistency across states; and to accommodate state specific resources, relationships, and other environmental factors to optimize efficiency and synergy with existing HIE initiatives.

Within this framework, the state teams used the following methods to complete the work; (the number of state teams that used the method is indicated in parentheses):

- formed core team and steering committee to oversee the project, provide feedback on products, and provide internal sign-off on deliverables (34);
- conducted face-to-face work group meetings (34);
- communicated via web mail, Internet, Wiki sites, Listserv (12);
- conducted one-on-one interviews (12);
- held teleconferences (10);
- conducted focus group sessions (8);
- held special events to engage consumers, providers, and other stakeholders (6);
- conducted regional meetings to engage stakeholders (4);
- conducted informational and “listening” sessions (4);
- communicated in hard copy (ie, newsletters, fliers, targeted mailing list) (4);

- leveraged existing health information technology (HIT) work groups (4);
- conducted WebEx or Condensor serve interactive type meetings (2);
- mailed surveys to participants who missed meetings (2);
- subcontracted for the outreach coordination (2);
- developed and launched external communication strategy (1); and
- used Survey Monkey for stakeholder feedback (1).

4.4 Regional Meetings

Achieving consensus among a representative group of stakeholders across an entire state or territory on the assessments of variations, barriers, and solutions was an ambitious task and was critical to the success of the project. To facilitate the exchange of ideas, 10 regional meetings were held. The key purpose of the regional meetings was to allow the participants to interact with a range of stakeholders from multiple states to discuss issues related to electronic health information exchange. The meetings brought together the leadership and stakeholders from multiple states to discuss variations in law or practice that were identified as barriers to interoperability and to work to achieve consensus on an acceptable range of solutions. The regional meetings also provided an opportunity for state-level stakeholders to hear the perspectives of national experts and representatives from the federal government.

Since addressing privacy and security issues related to electronic health information exchange requires a true collaboration among all of the 56 states and territories, states that did not hold subcontracts were also invited to attend the meetings and to contribute to the discussions. Appendix E details the dates, locations, and attendance for each meeting.

4.5 Nationwide Meeting

To discuss and finalize a nationwide summary and synthesis of variation assessments and proposed solutions among all states, it was determined that a nationwide conference would be the most valuable forum. The nationwide conference brought together representatives from 43 states to review what they learned and to discuss the potential solutions and plans to implement solutions for the future. Topics for the meeting included those put forward at the regional meetings, and topics and recommendations received by the state subcontractors in response to a broadcast request for discussion topics and activities. The agenda for the nationwide conference is included in Appendix F. Meeting slides and materials that provide more details about that meeting can be found at www.rti.org/hispc.

5. CURRENT NATIONWIDE LANDSCAPE FOR PRIVACY AND SECURITY SOLUTIONS

Analysis of the activity reported by the state teams reveals an emerging pattern that reflects the roadmap from paper-based health information exchange to full electronic health information exchange at the state level. The variation in the level of analysis, identification of solutions, and the scope and content of the implementation plans is driven by the current placement of the state on the road to statewide electronic health information exchange. One of the determining factors in the identification and selection of these priority solutions and implementation plans across states was the stage of development, adoption, and implementation of health information technology and electronic health information exchange initiatives within the state.

To better understand the context within which states made these determinations, the following section summarizes and categorizes the stages of development of electronic health information exchange of states participating in the Privacy and Security Solutions project. The section does not attempt to identify all of the electronic health information exchange efforts currently under way in each state. Rather, it focuses on creating state summary profiles and clustering states into identified levels of electronic health information exchange development, so that a nationwide landscape of state efforts for privacy and security solutions can emerge.

Based on a review of several national efforts that, taken together, collected, analyzed, and categorized the developmental stages of state electronic health information exchange efforts, the following dimensions were identified, selected, and used to assess and summarize the HISPC states as follows:

- state HIT/HIE underlying infrastructure factors:
  - level of HIT adoption and electronic health records (EHR) implementation in health care organizations within the state;
  - regional or local multiorganization or single-organization HIT/HIE activities under way;
  - existing large payers with electronic health information exchange/claims submissions;
- statewide HIE planning efforts:
  - statewide assessment of needs and planning process organized, under way, or completed;
  - roadmap developed;
  - clear leadership and accountability demonstrated to sponsored initiatives;
- organization and governance for establishing a statewide HIE:
  - formation of statewide HIE initiative included in the HISPC recommended solutions;

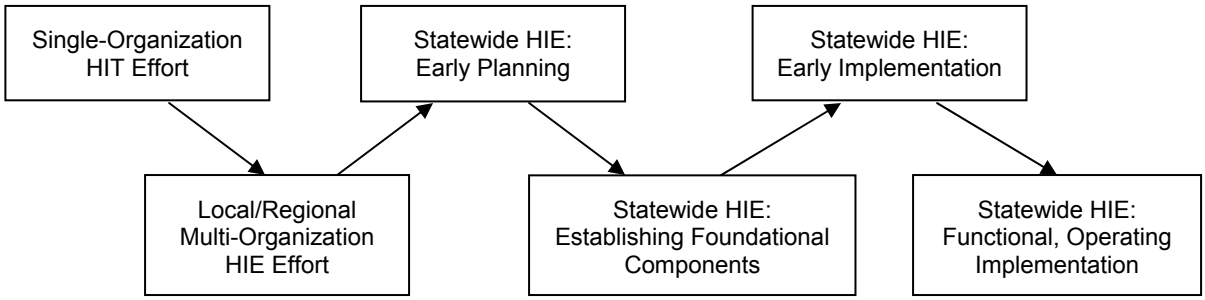
  - statewide coordinated HIE activity formally established;
  - coordinating organization identified to facilitate the process (independent entity, state agency, advisory board or committee, other organizing and governance structures);
  - website for statewide effort established;
- state government role:
  - state legislation passed or executive order issued for establishing a statewide HIE effort;
  - role of state government (eg, convener, facilitator, educator, funder, catalyst, partner, setting statewide HIE policy and standards, aligning the state programs and roles, ensuring statewide access to state HIE effort, acting as vehicle to reach and access multistate and nationwide efforts);
- funding and sustainability:
  - initial funding for statewide HIE initiative identified, secured;
  - financial model for ongoing funding and sustainability developed, adopted, and in place;
- implementation:
  - identification of HIE technology approach and definition of operating policies completed;
  - technology vendor(s) selection process under way, completed;
  - pilot project planned, implemented;
  - implementation of statewide plan getting started, under way;
  - level of statewide participation (providers, payers, government, consumers, others); and
- evaluation
  - project evaluation planned, completed; and
  - iterative review process on project for lessons learned.

Appendix G presents a summary of statewide HIE efforts in each state, the description and analysis of their various stages of development, whether an organization has been identified as the central coordinator/facilitator, the name of such organization, a website (if available) of the statewide HIE effort, and whether legislation to formally establish, authorize, expand or fund the central coordinator or the statewide HIE project itself was being recommended.

5.1 Overview of HIT/HIE Landscape of HISPC States

All participating states and territories have some type of electronic health information exchange activity currently under way. As shown in Figure 5-1, these activities range from independent, isolated HIT efforts conducted by one health care organization (single organizations), to the implementation of one or more local or regional multiorganizational HIE efforts, to the early planning of a statewide electronic health information exchange effort, to the establishment of foundational components of a statewide initiative, to early implementation of a statewide HIE effort, to more mature, operating statewide implementations.

Figure 5-1. Range of Current Electronic Health Information Activities Within States



5.1.1 Single-Organization HIT Efforts

All HISPC states have one or more single-organization HIT efforts under way. Many of these initiatives are undertaken and funded by the organizations themselves but in some cases, the initiatives are funded by state government, by private funders, or federal agencies, such as Agency for Healthcare Research and Quality's (AHRQ's) Health Information Technology Portfolio, which supports one or more HIT projects in 41 states. These organization-based private, state, and federally funded efforts have been instrumental in improving the electronic health information exchange capacity of local, small and medium-size health care provider organizations and, in many cases, rural and hard-to-reach-area health care providers, increasing the adoption and utilization of HIT by a wider and more diverse group of providers around the country, and addressing the technology gap between larger and smaller organizations. While much more work still remains, these funding and investment efforts are also contributing to better prepare the health care industry at the state, regional, and local level to participate in future statewide and national HIE efforts.

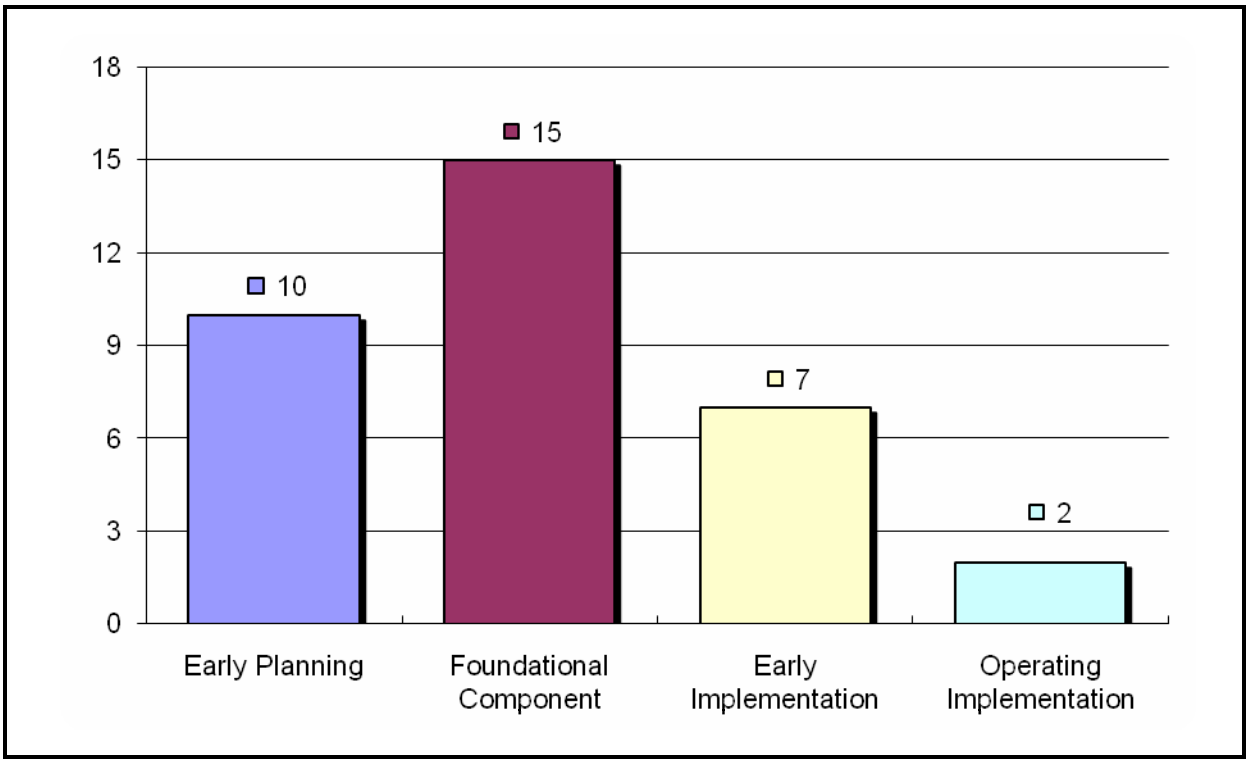
5.1.2 Local/Regional Multiorganizational HIE Efforts

For local or regional electronic health information exchange activity, all participating states identified one or more such efforts currently under way within their states. Most of these efforts are set in defined geographic areas in the state, are funded through local, state, private, or federal funding, and involve 2 or more provider organizations. Some states have done extensive inventorying of both HIT projects as well as interorganizational HIE initiatives.

5.1.3 Statewide Electronic Health Information Exchange—Early Planning

As shown in Figure 5-2, 10 of the 34 states are currently considered to be in the early planning stages of statewide electronic health information exchange development. This stage includes states that have not yet identified or established an organization to facilitate the statewide planning process, but have an agency or government body conducting preliminary assessment of HIT/HIE efforts in the state. This stage also includes states that

Figure 5-2. Distribution of HISPC-Participating States by Stage of Statewide HIE Development



have an identified government body or entity responsible for developing a statewide plan. Interestingly, several states completed such a plan in the 4 months between December 2006 and March 2007. In all cases where a plan had been developed, the plan covered governance and organizational issues, infrastructure and architecture options, and financial models (although in almost all cases, recommendations call for seeking and securing funding from state government). States in this group included Arkansas, Illinois, Iowa, Kansas, Mississippi, New Hampshire, New Jersey, Oklahoma, Oregon, and Puerto Rico.

5.1.4 Statewide HIE—Establishing Foundation Components

This stage of statewide HIE development include states that have (1) identified and established a central body to coordinate the HIE development; (2) appointed a governing body (board of directors); (3) established operating committees; and (4) completed a strategic plan or roadmap. A total of 15 states were at this stage of development, including Alaska, Colorado, Connecticut, Kentucky, Louisiana, Michigan, Minnesota, New York, North Carolina, Ohio, Vermont, Washington, West Virginia, Wisconsin, and Wyoming.

Here, too, the level of development varied within the group, both in how recently an entity had been appointed and a plan had been completed, to how comprehensive and final (vis-à-vis high-level and preliminary) the strategic plan or roadmap became. Nevertheless, these

states have devoted, based on the level of documentation available, a significant amount of resources and time in preparing, discussing, and reaching consensus on the plans.

Also, in most cases (9 out of the 14), the lead entity was a government body, a state agency, or a nonprofit created from the recommendations of a state body. In the remaining 5 states, the independent nonprofit organization was created by a community coalition of stakeholder group.

5.1.5 Statewide HIE—Establishing Early Implementation

In addition to the elements identified in the previous stage of development, in early implementation, the distinguishing factors were as follows: (1) some of the key roadmap implementation steps have been undertaken; (2) the statewide HIE initiative has selected a technology vendor; and (3) the state has began implementing HIE pilots. Seven states were classified in this category, including Arizona, California, Florida, Maine, Massachusetts, New Mexico, and Rhode Island.

In all cases in this group, the central coordinating body was a nonprofit entity. In 2 of the 7 states, the nonprofit organization was formally created via state legislation or executive order. The state government was identified to be an active participant engaged at the highest (Board) level of the nonprofit.

5.1.6 Statewide HIE—Functional/Operating Implementation

This group was characterized by a fully functioning statewide HIE effort, albeit the effort may only be supporting one or just a few types of clinical electronic health information exchange (ie, clinical labs, medications, note documentation, billing, claims scrubbing). Only 2 states, Indiana and Utah, were considered to be at this stage of development.

5.1.7 State Government Role

Across the board, state government roles in the planning and implementation of statewide HIEs varied from active participation to being a co-lead facilitator, to serving as the lead convener and providing initial funding support for the planning process and, in some cases, funding the initial infrastructure investment needed to launch the statewide HIE.

5.1.8 Financial Sustainability

For most states at a foundation level or early statewide implementation stage that have completed a statewide implementation plan, the financial plan called for a significant foundational support from state or federal government to launch the effort.

6. VARIATIONS, SOLUTIONS, AND IMPLEMENTATION PLANS

One advantage of looking across the work of the 34 state teams is that gaps in the work of some teams were filled by the work of others. So, for example, although gaps in knowledge about appropriate and required security practices were identified in many of the state team reports, a review of the 34 reports provides a more complete picture of the issues that need to be resolved, and approaches to those issues. This section provides a discussion of the key issues raised by the state teams, along with the proposed solutions and approaches to implementation.

6.1 Phases of Privacy and Security Solutions Project

6.1.1 Assessment of Variation

The American Health Information Management Association (AHIMA) was subcontracted by RTI to develop and test a set of 18 scenarios that provided a standardized context for discussions of organization-level business practices among stakeholders across 34 states and one territory (for a compilation of these scenarios, see Appendix C). In addition to promoting these discussions of business practices, the 18 scenarios were designed to promote discussions of policies and relevant state law across a broad range of stakeholders. The business practices identified during these focused discussions formed the basis for the assessment of variation in organization-level business practices. A list of the scenarios and the health information exchange purpose on which they were designed to focus are shown in Table 6-1. Although the focus of the project was ultimately to harmonize on best practices for electronic health information exchange, a significant amount of information could also be provided by examining current paper-based policies and practices and engaging in a discussion regarding issues that prevented entities from translating those policies into electronic equivalents.

As expected, a high level of variation was uncovered in the way issues of privacy and security were handled, not only among states, but at every level, even within a single practice. Undertaking a thorough analysis of this variation provided a significant opportunity for state project teams to start determining which variations were actually problematic to the sharing of health information under appropriate circumstances, and which necessary safeguards were required to support privacy and security. Reducing the variation around the appropriate transfer of personal health information will be extremely helpful as entities explore electronic health information exchange; agreements will be necessary regarding what data are transferred and how they are transferred.

Table 6-1. Purposes of Health Information Exchange and Relevant Scenarios

Purposes of Health Information Exchange	Relevant Scenarios
Treatment	Scenarios 1–4
Payment	Scenario 5
Regional health information organizations (RHIO)	Scenario 6
Research	Scenario 7
Law enforcement	Scenario 8
Prescription drug use/benefit	Scenarios 9 and 10
Health care operations/marketing	Scenarios 11 and 12
Bioterrorism	Scenario 13
Employee health	Scenario 14
Public health	Scenarios 15–17
State government oversight	Scenario 18

6.1.2 Analysis of Solutions

To ensure continuity between the assessment stage and the solutions stage, nearly all of the state teams included members of their Variations Work Group (VWG) and Legal Work Group (LWG) in their Solutions Work Group (SWG). Additionally, states added key members to their SWG through targeted recruitment of stakeholders with specific subject matter expertise. The composition of the SWG often evolved through time, depending on the knowledge and experience required to address particular issues and solutions. During the solutions process, several states merged their SWG with their Implementation Planning Work Group (IPWG), to achieve a fluid transition from solutions to implementation.

The state teams described an iterative process of solution development, review, validation, and refinement to identify and propose solutions. Additionally, the states described a vetting process for the proposed solutions that included review by the SWG, the LWG, the steering committee, the broader stakeholder community, consumers, and key government officials. To prioritize solutions, many states reported using a number of ranking, scoring, and weighting methods for seeking consensus during the priority-setting period.

In most states, preliminary determination of the feasibility of solutions was based on an evaluation of cost, ease of implementation, and time required for implementation. States were asked to make plans for solutions that could be implemented in the short term (12 to 18 months); therefore, not all solutions presented in the Assessment of Variation and Analysis of Solutions (AVAS) were included as implementation plans in this report. For the

most part, states created implementation plans only for solutions that were deemed feasible within the allotted time frame. Additionally, states generally selected solutions where they were able to identify key players and funding sources for their implementation plans.

6.1.3 Implementation Planning

As the state teams moved from identifying variation to creating solutions and implementation plans, they narrowed their focus and increased the depth of their analysis. To produce the plans, the state project teams followed a process that encouraged sharing observations, ideas, and concerns among an array of stakeholders including consumers, providers, insurers, state agencies, and others involved in health information exchange. The project teams in each state were encouraged to prepare short- and long-term plans to move from today's hybrid environment (paper and electronic) toward an interoperable electronic health information exchange environment based on common privacy, security, and technical standards.

6.1.4 Factors Affecting Variations, Solutions, and Implementation Plans

With the complexity of potential and actual exchange relationships, it is not surprising that the assessment of variation, development of solutions, and implementation plans varied on a number of key dimensions, including the following:

- Degree of adoption of electronic health information exchange. Several states pointed to sophisticated and functional systems of electronic health information exchange as models for expanding scale and coverage. However, many states lacked working models and, consequently, had to imagine issues and consequences of electronic health information exchange based only on experience with paper-based systems. And even in states where working models existed, coverage was far from universal. Many stakeholders in each state and across the country lacked practical experience with electronic health records (EHRs) and were unfamiliar with the concept.
- Health care market forces in the state. The business and organizational dynamics and relationships among health care entities differed across regions and states. Within states, specific markets were different, which affected the ways in which exchange practices were adopted and implemented.
- Legal and regulatory conditions related to health information. Relevant laws and regulations developed and evolved largely in response to the paper-based health information exchange. Legal restrictions addressing health information exchange were often dispersed across many different statutes and regulations and are sometimes inconsistent with one another. Several states reported that antiquated laws written for paper-only environments created significant barriers to electronic health information exchange. Other states noted that laws were silent with respect to certain aspects of health information exchange, leading to varied business practices and customs. In addition, differing federal regulations governing privacy and security affected practices related to health information exchange.
- Demographic composition of the state. Factors within each state such as population size, cultural and ethnic diversity, and geographic dispersion were considered in the development of implementation plans. In addition, several states considered interstate health information exchange in their plans, usually when they had

significant populations that traveled out of state for care, or when large numbers of tourists were present.

- Financial status of the state. Several states noted in their plans that funding of implementation plans was uncertain, and some states clearly indicated that the poor financial status of the state meant that resources were scarce and would not be devoted to electronic health information exchange.
- Cultural and historical characteristics. States varied widely in their approaches to privacy and security. Some had enacted laws that were very close to or equivalent to the "floor" of protections provided by the Health Insurance Portability and Accountability Act (HIPAA) Rules, while others had adopted far more stringent standards. In addition, historical events have shaped privacy standards, such as those for HIV/AIDS or genetic testing results.

6.2 Permission for Disclosure

Thirty of the 34 AVAS reports submitted by the state project teams cited significant variation in the business practices and policies surrounding the need for and process of obtaining patient permission to use and disclose personal health information. These variations were highlighted in the treatment, regional health information organization (RHIO), research, and marketing scenarios. Overwhelmingly, the state project team reports indicated wide variation among organizations in practices and policies that determine when patient permission is required, how the permission is obtained and documented, and how patient permission is communicated to health care organizations, payers, and other outside entities.

The state teams identified broad variation in the *need for* (perceived or otherwise) and the actual *process of* obtaining appropriate patient permission to disclose identifiable health information. Variation in application and implementation of obtaining patient permission was caused by a number of factors, primarily including

- a basic misunderstanding of whether and when the HIPAA Privacy Rule required patient permission to disclose health information, particularly with respect to treatment;
- confusion over the terms used for the process for obtaining patient permission;
- federal and state laws with patient permission standards that differed from the HIPAA Privacy Rule, particularly those that applied to *specially protected health information*; and
- organizational decisions to require patient permission as an added protection to reduce risk of liability for wrongful disclosure.

6.2.1 Consent and Authorization Under the HIPAA Privacy Rule

The HIPAA Privacy Rule specifically permits, but *does not require*, a *covered entity* to obtain written patient permission (called *consent*) for uses and disclosures of *protected health information* for treatment, payment, and health care operations. For those *covered entities* that choose to obtain *consent*, there is no requisite form for *consent* to share information for

treatment, payment, and health care operations under HIPAA. The content and format of *consent* to share information for treatment, payment, and health care operations is wholly within the discretion of the *covered entity*. The HIPAA Privacy Rule, however, does require patient permission to disclose health information for many purposes *other than* treatment, payment, and health care operations (called *authorization*). The HIPAA Privacy Rule prescribes specific content requirements for such *authorizations*. Significant confusion exists about these HIPAA Privacy Rule provisions; many people still believe that patient *consent* is required for treatment, payment, and health care operations, despite a wealth of information surrounding the HIPAA Privacy Rule disclosure requirements.[4]

Widespread confusion also existed about the terms used for obtaining patient permission. This confusion results partly from the HIPAA Privacy Rule's use of different terms and requirements for permissions that are related to different purposes: the term *consent* is used for written patient permission to use and disclose health information for treatment, payment, and health care operations, while the term *authorization* is used to describe patient permission to use and disclose health information for other purposes. Many organizations fail to make the distinction between *consent* and *authorization* under the HIPAA Privacy Rule and used the terms interchangeably. Adding to the confusion is the variation of terms in state laws, such as *consent*, *authorization*, *release*, and other terms to describe written patient permission to disclose health information.

State teams suggested a wide range of solutions to address the confusion stemming from the differing definitions and applications of patient permission. One of the most frequently cited solutions was the creation of a common or uniform permission form for both paper and electronic environments, to be used for treatment, payment and operations. State teams proposed 3 general designs for permission documents. The first option was a uniform permission form to be used by all. The second option was to offer a standardized permission form that includes certain elements, but may be modified based on institutional preferences. The third option was to provide model forms and allow institutions to draft their own forms. Each option has positive and negative aspects, including the amount of work required to achieve consensus on the content of the form, and the ability of the form to promote interoperability. While some state teams focused on uniform intrastate forms, some proposed the creation of forms that would be consistent across all states and the health care industry. Table 6-2 summarizes the benefits and weaknesses of the universal and model permission approaches.

[4] Some of this confusion may be the result of the *consent* provision's being amended between the publication of the Privacy Rule in 2000 and the Privacy Rule's compliance date in 2003. When it was originally released, the Privacy Rule required obtaining patient *consent* for treatment, payment, and health care operations. This provision was amended in 2002, and obtaining *consent* became optional.

Table 6-2. Benefits and Weaknesses of Approaches to Permission

	Benefits	Weaknesses
Universal Permission	Consistency Improved patient understanding Single body of case law can emerge Improved willingness to share information among providers	Difficulty in achieving consensus Providers may not like all elements
Model Permission	Improved willingness to share information among providers Flexibility and choice for providers	Inconsistencies arising from modifications made by providers

To implement their common or universal permission forms, state teams often turned to their new leadership bodies. As described in *Variations in Business Policies and Practices*, state teams recognized the need for an oversight or leadership entity to oversee the implementation of a range of solutions. Although these bodies were in various states of development—some were established, others were authorized by the governor or legislatures, and still others were in the planning stages—they were viewed as essential to implementing the state teams' solutions. The leadership bodies were to gather input from stakeholders, develop the content of the form, and roll it out. This process was to include educational efforts for stakeholders and possible legislative action to mandate use of the form.

One state team took a more comprehensive approach, outlining a *consent management process*. This process involves creating a leadership body, securing funding, drafting use cases, assessing policies and legal requirements, and educating consumers and providers. This is, by far, the most ambitious of the implementation plans related to *consent*.

Many states indicated that they wanted to maintain the requirement for patient permission but recognized that they would need to come to some agreement on a common approach to obtaining and managing patient permissions for information to be exchanged electronically. With this goal in mind, many state teams thought it would be useful to fully catalog state permission requirements (at least for treatment) and then work with other states having similar permission policies. States with similar permission policies may then be able to harmonize the variation in *consent* process requirements. The State e-Health Alliance for e-Health's Health Information Protection Taskforce is beginning to undertake some of this work.

State teams also suggested that national standards for permission might alleviate the confusion, either by generating more specific guidance on permission and release of information, or by creating a standardized data format that recognizes state-specific

requirements, but promotes interoperability at the national level. Specifically, the guidance should include clarification as to when a permission form is required, who must sign it, and make a clear distinction among the terms *consent*, *authorization*, and *disclosure*. These solutions offer an alternative to state-level work on permission, and may be necessary as states begin regional or interstate collaboration.

The Certification Commission for Health Information Technology (CCHIT) has indicated that it can accommodate some variation in *consent* laws, as long as they are "codeable." State teams will need to work with CCHIT and the Health Information Technology Standards Panel (HITSP) to ensure that their efforts are practicable in an electronic system. It became clear through the course of the Privacy and Security Solutions project that many state teams are unfamiliar with the work going on at the federal level, such as HITSP and CCHIT, and many teams are unfamiliar with developing technology for limiting access to or transmission of discrete health data. As the state teams continue to work through these issues, it will be beneficial to identify as models systems, both domestic and international, that are successfully using technology to facilitate patient permission choices.

6.2.2 Variation in Federal Law

States frequently cited the variation in the protection of health information under the HIPAA rules and other federal laws as a barrier to electronic health information exchange. Although these other laws did not appear to conflict with the HIPAA Rules, they often impose additional restrictions on the exchange of certain types of health care information, usually requiring patient permission for disclosure. In drafting the HIPAA Privacy Rule, the US Department of Health and Human Services (HHS) was aware of these more protective standards and intended to leave them in place.[5]

For example, several states mentioned the Family Education Rights and Privacy Act (FERPA), which governs most school records and has its own privacy and security regulations. Under FERPA's regulations, information contained in a school health record is considered an education record, which requires parental or student permission for disclosure, with the exception of health and safety emergencies (34 C.F.R. § 99.31).[6] State teams reported that this restriction unduly interfered with the exchange of school health record information for routine treatment purposes.

Another state team cited the Clinical Laboratory Improvement Amendments (CLIA) as problematic for electronic exchange of health information. One state suggested a revision to the federal CLIA regulations. The federal CLIA regulations, 42 C.F.R. § 493.1291(f),

[5] It should be noted that DHHS was aware of the restrictions of these other federal laws when drafting the HIPAA Privacy Rule and observed that "Congress did not intend for the privacy regulation to overrule existing statutory requirements in these instances." 65 Fed. Reg. at 82482.

[6] Note that the HIPAA Privacy Rule exempts from its scope these education records and certain other records that are covered by FERPA regulations.

currently provide as follows: "Test results must be released only to authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test." The term *authorized person* is defined in 42 C.F.R. § 493.2 as "an individual authorized under State law to order tests or receive test results, or both." The term *individual responsible for using the test results* is not defined in the CLIA regulations, and its meaning is uncertain. The state team proposed that the CLIA regulations may pose a barrier to laboratories' exchange of health care information directly with the patient, with HIEs, or with other similar organizations who may participate in electronic health information exchange. At least one other state proposed to review the CLIA regulations in light of HIE organizations that endeavor to provide electronic laboratory reporting services.

States also reported concerns with federal laws governing the confidentiality of alcohol and drug abuse patient records[7] and Medicaid information. These topics are more fully discussed in Sections 6.2.4 and 6.5. To address variations in federal law, state teams most often requested guidance from the appropriate federal agency.

6.2.3 Variation in State Law

Some of the variation in when and how patient permission is obtained is caused by varying state law requirements and organizational decisions to require permission as an added protection to reduce the risk of wrongful disclosure. Although the HIPAA Privacy Rule allows the disclosure of health information for treatment, payment, and health care operations without patient *consent,* some state laws require written permission for these purposes. In most states, the content of patient permission is not defined, leaving health care entities free to develop their own criteria. The lack of a standard permission form, even within a state, results in different health care entities' developing their own permission form requirements and refusing to honor permissions obtained by other entities, thereby interfering with the legitimate flow of health information.

One option to reduce variation is to amend state laws to be consistent across some dimension, such as aligning them with the HIPAA Privacy Rule. Multiple state teams proposed amending state law to include the treatment, payment, and health care operations exceptions included in the HIPAA Privacy Rule, align definitions across state laws, or create new definitions where none exist. The process for amending state law is relatively straightforward, although passing legislation requires a significant amount of effort, including outreach to legislators to promote the need for the change. Moreover, the content of the bill is likely to change as it moves through committees of the House and Senate. Implementation plans included outreach efforts to lawmakers and others with a vested interest in the outcome of the legislation, and noted the need for a considered approach, rather than attempting an overhaul of state privacy law. State teams often considered

[7] 42 C.F.R. pt. 2 uses the term *alcohol and drug abuse*. Most of the states used the term *substance abuse*. This summary has adopted the terminology from the federal regulation for consistency.

multiple options for amending state law, discussing the pros and cons of each choice and the expected impact on stakeholders, including providers, health plans, and patients.

6.2.4 Specially Protected Information

In general, the HIPAA Privacy Rule considers all personal health information equally sensitive and, with the exception of psychotherapy notes, permits personal health information to be used and disclosed for treatment, payment, and health care operations without patient *consent*. In contrast, a variety of federal and state statutes and regulations (laws) afford heightened privacy protections for certain classes of information generally perceived as *sensitive* and requiring special protections.

States often cited, for example, variation between the HIPAA Privacy Rule and the federal law governing the confidentiality of alcohol and drug abuse patient records (42 C.F.R. pt. 2), which generally requires the patient's *permission* for disclosure of information, including for treatment (except in emergency circumstances) and prohibits a health care provider or plan that receives such information from redisclosing that information without patient *permission*.[8] Because of the breadth of applicability of 42 C.F.R. pt. 2, little variation existed in the requirement to obtain permission to disclose this information between states. Rather, the variation centered on the differences between the HIPAA Privacy Rule's permissive approach toward sharing health information for treatment, payment, and health care operations, and the restrictions of 42 C.F.R. pt. 2, particularly in the treatment context.

In the majority of states, increased protections also exist for many other types of data in addition to drug and alcohol abuse records, including HIV/AIDS, mental health, and genetic information. These protections, which often require patient permission for disclosure, vary from state to state.

Although broad support exists for the additional protections afforded *sensitive* information, some major issues may impede the exchange of information both within states and across state lines. First, several state teams reported general confusion about how to handle *specially protected health information* in accordance with these federal and state laws and business practices. Second, from a practical perspective, most current EHR systems in this country do not include functionality for segregating *specially protected health information*. As a result, many states reported that they simply do not electronically transmit *specially protected health information* that requires specific permission for disclosure. Only 6 states discussed technical solutions for integrating *specially protected health information* into electronic health information exchange systems. One solution was to require opt-in/opt-out procedures for patients and methods for capturing and transmitting that information within

[8] Although 42 C.F.R. pt. 2 applies only to *federally funded* programs, this term is broadly defined and most alcohol or drug abuse treatment providers must comply with the regulation. In addition, most other providers in this field require a patient's *consent* before disclosing clinical data due to either ethical obligations or liability concerns.

and between systems. Technology-based solutions to segmenting these data included the use of filters to suppress data access to end users, increasing layers of computer security, using flags within databases to identify *specially protected health information,* and notifying end users that some *specially protected health information* has been blocked. One state recommended adopting the Continuity of Care Document as a technical means for facilitating the exchange of *specially protected health information* for treatment while limiting its use and disclosure for other purposes.

As mentioned previously, one option for reducing confusion related to permission is to create a universal or model permission form. This can also be applied to *specially protected health information*, and one state team proposed drafting a separate form to apply to all classes of *specially protected health information*. A single permission form for the release of *specially protected health information* offers the same benefits as a uniform or common permission form for general personal health information, although it may be more difficult to achieve consensus on the content of the form because of the information. Again, this solution would be implemented by the leadership entity, and would include education for patients and providers.

With respect to the 42 C.F.R. pt. 2 regulations, one state suggested that HHS should explore "the contours of *consent* without the need for legislative action" although they also recognized that their suggestion may require Congressional action. The team also recommended that HHS more clearly define 42 C.F.R. pt. 2 so that a single *consent* would allow for unlimited downstream releases for certain purposes and clarify that *consents* can describe generally the entities to which pt. 2 records may be disclosed. State teams also suggested that 42 C.F.R. pt. 2 could be amended to provide that patient *consent* is not required to exchange the data for treatment purposes only. As noted previously, state teams did not develop implementation plans for these solutions, as authority rests with the appropriate agency.

Although stakeholders respected the need for policies and procedures to protect personal health information, they also expressed a tension between access to appropriate health information being available to providers at the time it is needed, and security policies and practices that make that access useable while respecting the privacy of the patient.

Even if advances in technology and breakthroughs in workflow allow for easy segregation of data in EHR systems, specially protected information varies from state to state, making transfer of this data difficult. A state that requires segregation of genetic information would have to filter data received from a state that may not require data to be separated from the other health information of an individual needing treatment. There are potential solutions to these problems, especially as health care organizations replace their legacy systems. Canada has systems in place that allow "masking" of data, and is developing a system to negotiate the varying *consent* requirements between jurisdictions.

The state teams made it clear that the interplay among the HIPAA Rules, other federal laws that create specially protected classes of information, and state privacy laws has created a complex environment where it may not always be clear what is required. Some state teams, taking an approach that seems straightforward, have called for giving all health information a heightened degree of protection, which would raise the privacy bar but reduce the variation.

6.2.5 Variation in Internal Business Policies and Practices

Notwithstanding legal requirements, many providers and other *covered entities* require patient permission to disclose personal health information for treatment, payment, and health care operations to satisfy professional ethical requirements or for risk management. In fact, the state teams reported that most stakeholder organizations that participated in the Privacy and Security Solutions project required patient permission for treatment purposes, even if federal or state laws did not require such permission. Many state teams, for example, indicated that, while sexual health information is not part of a legally protected category, with the exception of HIV/AIDS status, most providers attach additional protections to sharing such information to protect their patients' privacy. Although variation in the requirement for and content of patient permission to disclose is due largely to state law and organizational practices, "HIPAA" is often cited as the basis for requiring patient permission for treatment.

The HIPAA Privacy Rule is a federal "floor" of privacy protections and thus allows other laws to provide more stringent privacy protections. Because privacy has been an important political issue for many years, many more stringent state and local laws have been enacted, typically for particular situations involving socially sensitive topics, such as mental health and sexually transmitted diseases (*specially protected health information* is discussed in greater detail above in Section 6.2.4). Understanding the complex interactions among the many laws, regulations, and local business practices governing health information privacy can be difficult.

Additional confusion occurs because the HIPAA Privacy Rule is generally permissive about *disclosures;* that is, the Privacy Rule requires disclosure of health information only when access to the information is requested by the patient and when it is requested by HHS for purposes of determining compliance. This position allows any local business practice to restrict health information sharing further, even when it is not supported by any law or regulation; information sharing is complicated, even for those who want to share health information for good reasons.

Although common or universal permission forms will reduce some variation, changes in business policies and practices will require education and leadership. To address the need for leadership, state teams planned a variety of oversight bodies and governance structures.

The HISPC process represents the first steps toward a coordinated effort to understand and facilitate electronic health information exchange. States often have scattered electronic health information exchange initiatives throughout the state, but lack an oversight body to coordinate those efforts. In states that are in the early stages of electronic health information exchange development, an oversight body will foster adoption of privacy and security policies and consistent standards. There are 3 general types of implementation plans for leadership and governance: those that call for the creation of a new oversight body; those that plan to leverage existing efforts or bodies; and those that plan to create smaller governance structures, such as committees to oversee specific topics (ie, technology standards or educational programs).

Twenty-two states identified solutions based on issues relating to leadership and governance, and 11 suggested forming a permanent committee or organizational body within the state to help oversee and guide the development of electronic health information exchange, as well as the implementation of privacy and security solutions. These bodies would play a significant role, including developing and monitoring standards for the state, providing education on privacy and security laws, and addressing needs across jurisdictional lines. Many of these state teams also proposed solutions that involved interaction with their state legislature, such as providing recommendations to state legislators and policy makers, and working with the governor's office to draft and pass legislation. By promoting consistent standards and policies, the leadership bodies will assist in reducing variation because of business practices.

6.2.6 Consumer Participation

State teams considered consumer participation an essential component in achieving health information exchange. State teams noted that patients often did not understand the content of the permission form or notice of privacy practices (NPP) that HIPAA *covered entities* are required to provide to individuals. The teams identified a need for single-page forms in easy-to-read language, as well as educational campaigns to alert consumers of their rights and responsibilities. With respect to electronic exchange, states planned to examine whether *opt-in* (asking patients if they would allow their information to be shared) or *opt-out* (telling patients that their information would be shared unless they requested otherwise) was a more effective method for obtaining participation in an HIE. State teams planned to conduct pilot programs to determine which method was more effective for balancing high participation rates with consumer privacy concerns.

These solutions were also usually assigned to the leadership body. Some of the bodies included an education or outreach subcommittee that would lead the educational efforts. Educational campaigns for consumers were often described in broad terms, and included a variety of topics, such as the benefits of electronic health information exchange and EHRs, and consumer rights and responsibilities.

6.3 HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards for the protection of certain health information. The Privacy Rule standards address the use and disclosure of individuals' health information, as well as standards for individuals' privacy rights to understand and control how their health information is used. The Privacy Rule is administered by the HHS Office for Civil Rights (OCR). The HIPAA statute was passed in 1996, and the Privacy Rule was finalized in 2002, with a compliance date for most *covered entities* of April 14, 2003.[9]

States reported many business practice variations based on different interpretations and applications of the requirements of the HIPAA Privacy Rule, which are discussed in Section 6.2. This section summarizes some examples from the state teams regarding HIPAA Privacy Rule issues that pose challenges to electronic health information exchange.

6.3.1 Flexibility in the HIPAA Privacy Rule and Interaction With State Law

The HIPAA Privacy Rule is generally designed to allow *covered entities* considerable flexibility in the policies and practices they adopt. Similarly, other federal and state laws tend to be drafted at a high level of generality to allow for considerable flexibility. While such generality is desirable and probably unavoidable, given the great diversity in size, financial and technical resources, capabilities and operational needs of health care organizations, it has had the unintended effect of generating significant variation in the application of both the HIPAA Privacy Rule and state law. In addition, organizations are uncertain about whether their own standards, or those of their exchange partners, will be considered legally adequate. Because HIPAA does not preempt more stringent standards, states have a wide variety of protections for personal health information. Some are at, or very close to, the floor of the HIPAA Privacy Rule, while others impose much more restrictive measures.

State teams recommended 4 general categories of solutions to address the variation caused by differing applications of the Privacy Rule and state law:

- education;
- standard policies and practices;
- creation of a compendium of state law, federal law, case law, and preemption analysis; and
- requests for federal guidance.

Many state teams observed that additional education about the HIPAA Privacy Rule is needed, as evidenced by the widespread misunderstandings among providers. State teams planned to offer additional education for providers, perhaps as a continuing education requirement. The educational programs are to cover differences in state law and the HIPAA

[9] Small health plans, defined as health plans with annual receipts of less than $5 million, were not required to comply until April 14, 2004.

Rules affecting electronic health information exchange; public misconceptions of the HIPAA Rules; specific topics requiring education, such as use and disclosure of information to personal representatives; and definitions of terms as they apply to paper and electronic environments. States should examine the relative successes of past educational programs before creating new ones.

Standard policies and practices are another potential solution. State teams suggested creating policies that address routine exchanges of information, both in regular and emergency circumstances. These exchange models would comply with both the HIPAA Rules and state law. The policies and practices would have to be developed by the appropriate leadership body and be reviewed by a variety of stakeholders. Once developed, the body would disseminate the policies and offer educational programs to explain their significance and implementation strategy. This may prove useful in certain circumstances, but may be less feasible, given the wide range of circumstances and situations that organizations face.

Many refer to "HIPAA" when describing privacy and security issues, even though state law and business practices are just as likely to pose challenges to electronic health information exchange. In addition, state law and the HIPAA Rules often have different requirements, leaving *covered entities* confused about how to comply. State teams proposed amending the definitions found in state law to reflect those found in the HIPAA Rules. Aligning definitions will facilitate legal analyses and reduce uncertainty. Alternatively, states also suggested compiling a compendium of relevant state law, federal law, case law, and preemption analysis. State privacy laws were generally passed over time and are frequently scattered throughout many chapters of the state code. Case law may also contain conflicting interpretations. Part of the complexity is driven by the fact that HIPAA does not preempt more restrictive state law. Thus, *covered entities* must comply with both the HIPAA Privacy Rule and these more restrictive state laws.

Federal guidance could take a number of forms. States requested that OCR publish de-identified case studies that describe what sort of privacy lapses were identified and what corrective action was taken. It is important to note here that OCR now publishes specific but de-identified case examples of corrective action obtained from *covered entities* through enforcement of the Privacy Rule. One state team felt that the additional protection provided to "psychotherapy notes" did not offer enough detail and requested further clarification. State teams also felt that further guidance regarding *de-identification*, *limited data sets*, and *designated record sets* was necessary to address confusion in these areas. Finally, a state team requested that OCR add information on HIT to the frequently asked questions section of its website.[10]

[10] Resources from OCR can be found at its website (OCR, 2007, June 29).

6.3.2 Business Associate Agreements

The term *business associate* is defined in the HIPAA Privacy Rule and refers to a person or entity that performs certain services or functions or to activities involving the use or disclosure of personal health information on behalf of a *covered entity*.[11] These functions include "claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing." The services include "legal, actuarial, accounting, consulting, data aggregation . . . management, administrative, accreditation, or financial services." In addition, *covered entities* can be a business associate of another *covered entity*. The Privacy Rule requires that a *covered entity* obtain satisfactory assurance from its business associates that they will safeguard personal health information. This assurance must be in the form of a contract or other written agreement.

Often exchange between entities is undertaken pursuant to a Business Associate Agreement (BAA).[12] Although these agreements allow for the exchange of identifiable patient information, they are typically created on a case-by-case basis and, therefore, contain a large amount of variation themselves. In addition, BAAs are not used consistently. Many state teams believed that BAAs are necessary to exchange health information for treatment, although the HIPAA Privacy Rule does not require such an agreement for a *covered entity* to disclose information to a provider for this purpose.

One of the most frequently cited solutions to the inconsistent use of BAAs was to draft model agreements, combined with educational materials. State teams also recommended that electronic health information exchanges offer model BAAs tailored to the exchanges between providers and the electronic health information exchange. Some states also proposed making a BAA mandatory for information exchange. In such cases, the state teams felt that passing state law to require a BAA was a sound policy and would promote exchange by reducing mistrust and liability concerns.

The model agreements would be developed by the state-level leadership entity, a state agency, or the leadership of an electronic health information exchange. OCR has published sample business associate contract provisions, which could serve as a foundation for states that wish to create model agreements. Once a model agreement was created, states would publicize its existence through the entity that created it or via professional organizations. In this respect, model BAAs may prove most valuable in the context of an established HIE. By requiring a BAA for participation in an electronic health in formation exchange, providers

[11] See 45 C.F.R. § 160.103.

[12] None of the states used the more specific term *business associate contract*. The Rule has specific provisions for business associate contracts and other arrangements. The other arrangements category includes, for example, memorandums of understanding between agencies. Because the term *business associate agreement* encompasses both contracts and other arrangements this term is used in the summary above.

can be confident in the privacy and security practices of the other participating organizations. Although *business associate* is defined under the HIPAA Privacy Rule, state teams felt that BAAs were a valuable tool that could also be implemented at the state level to address circumstances where the definitions found in the HIPAA Privacy Rule do not apply.

6.3.3 Minimum Necessary

The most common source of variation reported related to the HIPAA Privacy Rule is the interpretation and application of the *minimum necessary* standard. The HIPAA Privacy Rule states that "a covered entity must make reasonable efforts to limit *protected health information* to the *minimum necessary* to accomplish the intended purpose of the use, disclosure, or request" (45 C.F.R. § 164.502(b)). The *minimum necessary* standard was intended to be flexible and scalable to accommodate different health care settings and needs.

The state teams reported widespread variation in how the *minimum necessary* standard was understood and applied (ie, applying the *minimum necessary* standard varies from situation to situation). The level of information provided to satisfy this standard varied not only from organization to organization, but also between people within the same organization. Many states suggested that this variation was more a problem of differing applications and interpretations than a true legal barrier.

An example concerning the *minimum necessary* issue is access to electronic data by outside entities, specifically payers. The state teams reported that hospitals currently do not allow third-party payers access to their EHRs, and access by nonhospital personnel generally is restricted and often limited to hard copies of medical records. EHRs generally do not allow for data to be segregated, and sending the entire record would violate the *minimum necessary* rule, although it would facilitate claims processing. Payer stakeholders agreed that if they did not already have the information they were seeking through their own claims data, they would request the additional information using a paper-based procedure for release of information.

While the states agreed that disclosures relating to payments are exempt from the HIPAA Rule's *authorization* requirements, stakeholders were confused about what amount of patient information meets the *minimum necessary* requirement. States were also concerned about the ability to segregate information in an EHR to meet the *minimum necessary* requirement. States that were unable to segregate the data felt that they would be stuck in an "all or nothing" situation when sharing data, and therefore, would not share any data electronically for fear of improperly disclosing information. The issue of granting access in a HIPAA-compliant manner was a concern commonly reported by the state teams.

Stakeholders experienced in electronic health information exchange indicated that most EHR systems do not include functionality for segregating health information. While most stakeholders respected the need for policies and procedures to protect personal health information, they also expressed a tension among access to appropriate health information being available to providers at the time it is needed, having security policies and practices make that access useable, and simultaneously respecting the privacy of the patient. Many stakeholders who were privately practicing physicians or part of a small group practice felt that the prohibitive cost of EHR systems that provided adequate levels of security was a significant barrier to electronic health information exchange.

State teams suggested a range of policy, technology, and legal solutions and implementation plans to address varying interpretations and applications of the *minimum necessary* standard. One option is to clarify and standardize *minimum necessary* data sets by role of accessing party, use situation, or both. For example, a payer might be given access to demographic information and diagnosis and treatment summary information for a given episode of care. Such a solution would require a review of the various requests that providers receive, as well as a method for obtaining additional information when the pre-approved data set did not meet the needs of the recipient. It is important to note that the HIPAA Privacy Rule already allows *covered entities* to develop standard protocols for routine and recurring disclosures to comply with the *minimum necessary* standard. State teams also noted a need for a system to transmit the information, suggesting a web-based transmission system or some other technology infrastructure. To improve existing systems, one project team also proposed designing hospital information systems with more sophisticated and systematic means of providing the *minimum necessary* information, although this requires additional collaboration and planning.

State teams also requested guidance from OCR as to what constitutes the *minimum necessary*, either in the form of standard policies or use cases. State teams also suggested that the *minimum necessary* standard be reviewed in light of electronic health information exchange, and that technical adjustments should be made. It is not clear at this time what technical adjustments might be required, given the inherent variability as to what constitutes the *minimum necessary*.

6.3.4 Covered Entities

Covered entities are defined in HIPAA (the Act itself) and in the Privacy Rule as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards (see 45 C.F.R. §160.103). The Privacy Rule applies only to *covered entities*; it does not apply to all persons or institutions that collect individually identifiable health information. Therefore, many stakeholders reported a fear of providing personal health information to entities that may not be held to the same standards of privacy under HIPAA

because of their questionable covered entity status, especially regarding redisclosure of that information.

The states reported variation in the definition, role, and status of RHIOs[13], particularly related to data collection, analysis, and disease management. Several state teams were unsure of a RHIO's legal status in their state, and opinions differed about whether a RHIO was a HIPAA-covered entity. One state mentioned that a RHIO had no uniform definition, nor was a RHIO recognized as a specific legal entity in the state. The general consensus among provider and hospital stakeholders in states where a RHIO has uncertain status was that they would be reluctant to input information into the RHIO if it were not subject to HIPAA or state regulations. If a clarification determining legal status of a RHIO is not made at the federal level, states may have to pursue definitions within their statutes or risk substantial confusion among stakeholders as to the provisions of guiding such organizations.

State teams also questioned the covered entity status of organizations such as homeless shelters (mentioned in Scenario 17) and certain county health departments (Scenarios 15–17). Some health departments are *covered entities* because they are direct providers of health care services and conduct standard transactions, while others are not. The HIPAA Privacy Rule permits disclosures of personal health information to public health authorities without individual *authorization* "for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions" (45 C.F.R. § 164.512(b)). Although these disclosures are allowed, states found that many stakeholders were not comfortable submitting personal health information electronically to a health department or other noncovered entity without assurances that the recipient would only use the information in accordance with the policies of the originating organization.

States were at various stages of development with HIEs, which was reflected in the solutions and implementation plans. Some states have operating RHIOs, while others are considering launching an HIE, and still others are not yet ready to consider creating an HIE. In states where an HIE is under consideration, but has not been created, state teams are examining models for the exchange, and methods for handling access, authorization, and authentication of users. They are also attempting to ascertain the legal status of their HIEs, considering whether they might be *covered entities*, business associates, or another category that does not fall under the HIPAA Rules. One state team believes that the functions of their proposed HIE render it a clearinghouse as defined by HIPAA. Clearinghouses are defined according to the functions they perform (processing data from a

[13] State teams generally used the term *RHIO* in their reports. Analogous terms include *electronic health information exchange,* a more generic term than *RHIO* since it does not imply regionality, and *Sub Network Organization* (SNO), which implies participation in a larger network and also does not suggest regional confinement.

nonstandard form to a standard form or vice versa), and can include a variety of businesses; this designation may or may not apply to a given RHIO. State teams also plan to pursue legislation to authorize HIE roles, accountability and functionality, and to support the HIE financially by pursuing fundraising, grant opportunities, and government appropriations and identifying sustainable business models.

State teams are also considering legal solutions to address the issue of noncovered entities. One state has drafted an implementation plan to accredit HIEs. The accreditation process for HIEs would require minimum policies and standards for privacy and security, and state law would prohibit HIEs from operating without accreditation. Another state team took a broader approach, and planned to reach out to the State e-Health Alliance and the National Conference of Commissioners on Uniform State Law (NCCUSL) to explore options for legal standards for privacy and security for noncovered entities.

Federal guidance is another option for addressing the status of HIEs. State teams requested clarification of the HIPAA Rules that would specify that HIE organizations are business entities with which clinical information can be shared or would identify conditions under which HIEs would be considered *covered entities*. Because the term *covered entity* is defined statutorily, any changes to the definition would require Congressional action. As electronic exchange expands, privacy and security standards and definitions of those required to follow those standards become increasingly important because of the array of entities processing or storing information.

6.3.5 Appropriate Disclosure and Redisclosure of Protected Health Information

In setting standards for *disclosure*, the HIPAA Privacy Rule generally does not distinguish among the different sources of personal health information maintained by a covered entity. However, some state teams reported confusion about whether the rules for disclosing personal health information that had been received from another provider were the same as or different from that generated in-house. Frequently, information received from another provider is incorporated into an organization's internal medical records. However, some organizations limit the information incorporated into the record to information used in the course of treatment, while others incorporate the full range of information provided.

A number of state teams reported that stakeholders were unclear about whether a subsequent request for a patient's record should include the information obtained from the other organization. One potential source of this confusion may be state laws, some of which define a "medical record" as including only information generated in-house. Many organizations reported that they would disclose only patient data that were collected directly by the organization. In other words, many providers believe that they cannot redisclose another provider's records. In addition, some organizations were concerned that *specially protected health information* could be incorporated into the patient's record and then be

released downstream without appropriate permission. Most state teams recognized that the misunderstanding around re-release and redisclosure is a source of variation that will need to be addressed to permit widespread interoperable electronic health information exchange.

While the question of the ownership of health information looks simple, its answers are quite complex. The short answer is that the law is not always very clear in this area, so it is better to define *information access, use, disclosure and protection rights,* and *obligations* by agreement among the parties to electronic health information exchange, rather than rely on property laws and concepts.[14] In an EHR and electronic health information exchange environment, it is also crucial to recognize and reflect the important distinction between health information and records, and the medium containing them. For ownership of health information and medical records, property is more accurately described as a bundle of rights and obligations.

Paper is an inexpensive, easy-to-use, easy-to-obtain medium; as long as health information is stored on paper, it is simple and straightforward to keep it in the owner's possession and protect it against unauthorized access, as in a file room. Electronic media kept in the owner's facilities should also be relatively easy to keep and protect. However, once servers and other network components become the medium for record storage, possession and protection become more difficult. This may become especially problematic where information services are outsourced, so that another party owns and operates the medium in which records are stored. From a property perspective, a services-level agreement for outsourced information services is a form of lease, in which the owner of the records rents use of the vendor's systems. Because of the limited property right in records media provided by such an arrangement, contracts for outsourced EHRs and related systems must include provisions protecting the record owner's rights and ability to maintain continuous use, and transition to an alternative services vendor or system, when and if necessary or desirable. For this reason, states are considering mandating privacy and security standards for noncovered entities that routinely handle personal health information (see Section 6.3.4 for additional information).

Ethically and legally, health care providers must make health information available whenever needed for the patient's care; this obligation is based on the Hippocratic Oath, though it is codified into law in some states. Under the HIPAA Privacy Rule and a number of state laws, health care providers are also required to give patients access and allow them to have copies of the information in their records. HIPAA *covered entities* are also limited in the uses and disclosures they make with personal health information, and some state laws also impose comparable (if not usually coextensive) limitations. Correlative individual information access rights and information use and disclosure restrictions should be imposed

[14] Intellectual property law does not apply because legal protections apply only if the information is patented, copyrighted, or a trade secret. None of these provisions apply to health information.

on noncovered entity HIE participant through BAAs (or other agreements). At least one state (New Hampshire) explicitly makes the patient the owner of the information contained in medical records, though not the medical records themselves. The same general principle applies to records created by other kinds of entities too; the party that creates a record owns it, subject to any information rights of the data subjects and other legal access rights, such as subpoenas in litigation.

State teams offered several solutions to these concerns. One state team planned to examine the federal and state provisions governing ownership of and responsibilities to maintain and control patient data and records and, if necessary, recommend a consistent interpretation or application of ownership, stewardship, or custodianship (or some combination among the three) with regard to patient data and records. As noted previously, if providers are concerned about whether they should release information, they will usually decline to do so. Standard policies and procedures, as well as the implementation of safe harbors (described in more detail in Section 6.3.6) may reduce this variation, as will clarification of state law. As noted above, the legal concerns raised by the concept of ownership will require legal counsel and careful analysis.

6.3.6 Liability Concerns

Although some of this confusion may be mitigated by moving to electronic management systems, many situations call for professional judgment or a reasonable decision to be made on the basis of current circumstances. Several states raised the issue of perceived liability under these circumstances. Many of the state teams reported that fear of penalties and sanctions for violating the HIPAA Rule's provisions creates an environment where staff interpret disclosure rules restrictively, which sometimes prevents or interrupts health information exchange, even in treatment situations. This fear persists even though no civil monetary penalties have been imposed under HIPAA, and only 3 criminal convictions have taken place.

Fear of HIPAA sanctions is not the only source of concern. State teams reported concerns about federal regulations governing drug and alcohol abuse treatment records; state regulators who conduct reviews based on licensure; state licensing boards that license individual providers such as physicians, nurses, chiropractors, and others; litigation by patients; and negative publicity. Although all sources of liability are of concern to health care organizations, negative publicity was reported as a significant source because of the resulting damage to the "brand" of a health care organization. Such liability is difficult to measure and difficult to counteract. Negative publicity can also result in the loss of patient confidence, a reduction in the number of payers willing to do business with a provider, and a reduction in the value of goodwill and reputation that the provider has developed over time. Because liability for inappropriate or unauthorized disclosures of health information can result in significant loss that is not easily remedied, health care organizations are

cautious about exchanging data. When health care organizations have liability concerns about the exchange of information, the exchange will generally not occur. They want to be confident that any mechanism for health information exchange has adequately addressed privacy and security issues and minimizes their organization's liability.

One solution proposed by some state teams is the development of *safe harbors* for policies, procedures, and business practices implemented to address privacy and security issues. This particular solution is intended to reduce fears of liability associated with health information exchange, fears arising from the lack of legally recognized standards for many privacy and security policies and practices.

No state articulated a preference for legal mandates specifying standards, which would be difficult to develop in sufficient detail and likely to become obsolete or fail to apply appropriately in some cases. Instead, some states proposed the establishment of legal safe harbors for policies, procedures, and practices that had widespread acceptance—consensus best practices, as identified by the community, and to be implemented by a new leadership body, or appropriate state agency.

For best practices to become safe harbors, appropriate legislation must be passed, authorizing some agency to adopt identified or recommended best practices as safe harbors through a regulatory process. Precedent exists for this process at the federal level with the Stark and anti-kickback laws, which are so potentially broad in application that they could be construed to criminalize many legitimate, even valuable financial arrangements and transactions. In response to this concern, Congress authorized HHS to publish exceptions and safe harbor regulations, specifying arrangements and transactions that would not be considered violations of the law.

A privacy or security policy or practice adopted as a safe harbor would not be a legal mandate—no penalties would be levied for failing to adopt it, so organizations that did not find it appropriate would not have to adopt it. However, if an organization did adopt the policy or practice, and subsequently experienced a privacy or security problem or failure that arguably could have been prevented by adoption of an alternative, the organization would not be subject to penalties or other liabilities. Once the safe harbor became effective, health care organizations that adopted the policy and practices would be assured that regulatory authorities would find it legally compliant and not penalize them in case of an investigation of their compliance. The organization could also rely on it as the standard of care in case of litigation, including allegations that the organization provided inappropriate access to information. Finally, the organization could permit electronic health information exchange transactions with individuals associated with their business partners that had also adopted the safe harbor policy and practices with confidence that these transactions also complied with the law. The safe harbor would, therefore, create an incentive to adopt interoperable policies and practices, without specifically requiring anyone to do so.

This kind of safe harbor scheme will take some effort to implement and manage. It would require development of both community processes to recommend policies and practices, and agency authority and operational structures. It is not clear that HHS would have the authority to implement safe harbors under HIPAA, though the question merits analysis, and federal safe harbors would not apply to state laws. Conversely, state agencies would not have the authority to implement HIPAA safe harbors. Nonetheless, given the potential this solution has to create incentives to overcome a substantial number of barriers through an open, public process, such efforts might prove quite valuable.

6.3.7 Accounting of Disclosures

State teams also identified the issue of accounting for certain disclosures, as is required by the HIPAA Privacy regulations, as an unnecessary burden not consistently implemented by organizations and not well understood by patients and consumers. The HIPAA Privacy Rule requires *covered entities* to furnish an individual, upon request, a written accounting of certain disclosures that have been made within the prior 6 years (see 45 C.F.R. § 164.528). Disclosures for treatment, payment, and health care operations, to the individual, pursuant to *authorizations* and others are exempt from this requirement. Although not directly a barrier to electronic health information exchange, states stated that this accounting requirement has created confusion and added burden to the process of health information management. The following main issues were reported.

- Significant confusion remains about which types of disclosures must be documented and to what extent.
- Organizations have invested significant resources in creating a mechanism to document such disclosures, and organizations continue to invest significant resources in maintaining such systems.
- Consumers have not used these systems or used them rarely (only on very rare occasions, do consumers request an accounting of disclosures).
- Even when consumers request such accountings, they soon realize that the information recorded in an accounting is not the type of information they were seeking.
- An assessment of consumer desires and an examination of what is operationally feasible in accounting for disclosures would provide a useful framework for any subsequent federal changes to the current HIPAA Privacy Rule accounting requirements.

6.4 HIPAA Security Rule

Confidentiality, integrity, and availability are the backbone of health information security. To support all 3 characteristics, security must be implemented as a careful balance of administrative, technical, and physical safeguards tailored to the particular information systems environment of each installation. This is best done through a risk assessment of the information systems environment followed by ongoing risk management through the

selection, implementation, and monitoring of reasonable and appropriate measures to minimize the risks while controlling the costs. The HIPAA Security Rule was specifically designed to be flexible and scalable because electronic security is dynamic. Security threats arise frequently, and their specific solutions evolve quickly. The flexibility and scalability of the Security Rule takes this into account.

Often these measures involve policies, procedures, and contracts with business associates more so than technology. Because the majority of security breaches are internal, if security technology is to work, behavioral safeguards must be established and enforced. Success requires administration commitment and responsibility at the highest executive level in an organization. Without this top-down commitment, any security measure is likely to fail.

The HIPAA Security Rule became effective on April 21, 2003, and was created to establish a minimum standard for security of electronic health information exchange. The standards require *covered entities* to implement basic safeguards to protect electronic *protected health information* from unauthorized access, alteration, deletion, and transmission.

Unlike the HIPAA Privacy Rule, which applies to both paper and electronic *protected health information*, the HIPAA Security Rule applies only to *protected health information* in electronic form. In most states, clinical data are still in paper form and, therefore, patient information is exchanged informally by entities, most often verbally and by fax. In this context, state teams found that security policies were unevenly implemented in practice. Stakeholders tended to rely heavily on already established relationships when they exchanged information, with voice recognition alone serving as the means of authenticating the person receiving the information.

The HIPAA Security Rule sets very general principles that apply to *covered entities* maintaining *protected health information* in electronic form. However, because HIPAA gives each organization the flexibility to implement security in a different way, implementing security when exchanging *protected health information* between organizations requires a more well-defined, standard set of mechanisms than when exchanging among known and understood electronic systems under the control of a single organization. Also, other laws and regulations could complicate the situation by adding security requirements that do not necessarily conflict with the HIPAA Security Rule but are different in different situations or locations. Fortunately, very few such situations exist.

However, the fact that the HIPAA Security Rule only provides general guidelines and expects each organization to conduct periodic risk analyses and implement measures that are “reasonable and appropriate” leaves much to local interpretation and variation. Because security risks and measures change rapidly over time, the asynchronous implementation of measures can also complicate the ability to exchange information between organizations. HHS recently issued some guidance in this area, but it is still quite general. For example, technological measures to counter the increase in the theft of portable devices (media

encryption) and remote access attacks (2-factor authentication) have become available in cost-effective forms; however, no industry-wide standard exists about how and when to implement them.

Results from this project indicate wide variation in the interpretation and implementation of the HIPAA Security Rule, with state teams identifying broad variation among stakeholders regarding appropriate security policies, procedures, and technical solutions. State teams found that legal standards for security are lacking at the state level and are generally not perceived to be sufficiently adequate or specific. Sharing personal health information among institutions requires a significant degree of trust in the technology, and in the other organizations' ability to implement it. State teams found that providers were worried that entities receiving their data might not have robust security measures (as robust as the providers' measures), and that this difference might expose them to liability in case of a security breach. Related to this concern was a lack of understanding that security in health care is far more complex than just the adoption of appropriate technical standards.

Thirty-one state teams offered technology-based solutions to security issues. The level of specificity in the solutions varied widely, from general statements that certain technical issues would have to be resolved to achieve an acceptable level of security, to very specific and detailed discussions of how to resolve specific issues. For example, one report provided specific technology-based solutions to security issues encountered during the creation of an electronic health information exchange program in their state, including user/entity authentication, access control, patient and provider identification, specially protected personal health information, protocols for information transmission, audits, and use and disclosure policies.

State-level implementation plans clustered around several topics, including identification of patients and providers; authentication, authorization, access control, and audit (the 4 A's); secure transmission of *specially protected health information*; and standards and best practices. One state team suggested implementing a plan for 3 sets of standard policies and procedures that would meet the HIPAA Security Rule compliance requirements. The standards would be based on the size of the provider (small, medium, and large), and each provider would be given generic templates as guidelines. Then, each entity would be responsible for implementing security measures that were "reasonable and appropriate" to them (ie, in line with the HIPAA Security Rule standards). Other state teams will be implementing education and training programs in electronic health information exchange and privacy and security for providers and their staff.

6.4.1 Authentication, Authorization, Access Control, and Audit

The 4 A's—authentication, authorization, access control, and audit—are an integral part of secure electronic exchange. Data security emerged as an important issue in almost every discussion about electronic health information exchange technical issues.Twenty-three state

teams addressed issues related to one or more of the 4 A's. While some discussions were fairly general, others outlined very specific solutions. For example, one state developed a set of 19 principles regarding the 4 A's that were specific enough to assist organizations in making decisions regarding electronic exchanges, yet flexible enough to adapt to future changes in the implementation of electronic exchanges.

Taken together, the 4 A's form the backbone of electronic health information exchange. These 4 components help ensure that personal health information is accessed by, and for, the appropriate individuals and for legitimate purposes. State teams proposed a wide range of implementation plans and pilot projects around these issues, including: the use of clearinghouses to authenticate users; the use of biometrics; stronger password protections; role-based access; software tools to determine the *minimum necessary;* digital signatures; and technology that would alert users to suspicious activity. In their implementation plans, state teams also proposed to address the user aspect by considering a framework for technology policies, assessing the impact on workflow, and increasing manual oversight.

Authentication

For the purposes of this project, *authentication* was defined as *the ability to verify that a person or entity seeking access to personal health information is who he or she claims to be.* At least 19 states included a discussion of authentication issues for data security. One significant issue was the lack of standards for authentication among all entities involved in a data exchange. In the absence of generally accepted authentication standards, stakeholders were unable to trust that personal information would only be provided to, or accessed by, the correctly identified users. In many circumstances, voice recognition, caller-ID, and requests received on letterhead were cited as the means for authenticating the individuals on the receiving end of the personal health information.

A solution often proposed was the creation of standard policies and procedures to be used by all participating organizations. Other solutions included the use of technology, such as digital certificates, biometric authorization, and role-based access control to ensure an appropriate level of security during the transfer of personal health information. One state is developing an interoperable infrastructure to facilitate sending and receiving electronic health care messages. Although this state anticipates a central identity verification method, individuals attempting to log in and use the system will first be authenticated through their home organization. Participating organizations will be responsible for maintaining a list of employees or affiliated individuals to ensure appropriate access. This approach requires each participating organization to abide by standard authentication methods to be granted access.

Implementation plans recommended that a committee be formed within the state to create standard authentication policies and procedures. States suggested including members of major health care providers on this committee to help with the approval and agreement

process for implementing these standards. The impact of this plan could be measured by the number of providers that adopt the committee's policies and procedures.

Authorization and Access Control

Information authorization and access control issues were often raised in tandem. Appropriate authorization policies and procedures are necessary to ensure that personal health information access rights are only granted to approved individuals, entities, or software programs, and only for purposes permitted by law and organizational policy. Consumers, and persons responsible for maintaining their data, are concerned that the level of information shared among individuals or entities is appropriate, and also that the individuals receiving the information are appropriately authorized to view the data. The state teams noted that, although variation exists among providers about the use of electronic records, providers who are already using EHR systems employ measures such as log-in names and passwords to limit access to electronic information to approved users only.

Role-based access helps ensure users have access only to the information that they need, not the entire EHR. However, many hospitals have role-based access criteria only for their own facility, which is often not compatible with other facilities, creating variations in authorization and access to EHR. Additionally, state teams found that role-based access has no community standard for permission levels that control access based on an individual's job responsibilities. The inability for current EHR technology to appropriately segregate data was also identified as a challenge to appropriate role-based access. In some cases, organizations are left with the decision to either permit internal access to too much information or to withhold information to a degree sufficient to hinder the job duties of a member of an organization's workforce. This problem was associated with technical inadequacies, which led to issues with allowing external parties electronic access to appropriate portions of the consumer's health record.

Many states looked to technology, as well as standard procedures and policies, as potential solutions for authorization and access control issues. One suggested solution to address access control was a universal role-based access scheme, with standard definitions for job titles and roles among those authorized to access the data. Each provider would be required to map internal roles to a set of standard roles. Individuals could view only certain parts of the data based on their job title or description, allowing for the separation of employees requiring access to clinical data from those requiring only administrative data access.

As with authentication, suggested implementation plans involved the formation of a state committee to set standard policies and procedures, as well as minimum security standards for electronic health information exchange. This committee would coordinate analyses of information technology (IT) security issues, conduct research around security standards, identify and adopt a set of electronic health information exchange security standards, and

recommend tools to ensure that IT security policies are consistently enforced throughout the state.

Audit

Information audits refer to policies, procedures, and system functions for recording and monitoring the activity of health information systems. The ability to create audit trail records related to the transfer of personal health information is a core building block for electronic health information exchange systems, as well as a requirement of the HIPAA Security Rule. An environment of trust will enable the secure electronic transmission of patient information. However, to create and sustain trust, verification processes are essential to monitor compliance with agreed-upon standards. Verification requires audit processes to track system usage and protect against inappropriate activity. To be consistent and effective across all providers, minimum audit requirements, policies on length of storage of audit records, and guidelines for controlled access must be established.

State teams reported that it was important to ensure that all organizations were monitoring the access of data by users as a safeguard against improper use, disclosure, or modification of personal health data. However, several state teams found variation in auditing capability among the stakeholders. Technical inadequacies and nonexistent or poor audit programs among some providers proved to be a challenge to electronic health information exchange. This challenge was especially true when personal health information was shared across networks or among multiple entities, particularly regarding inadequacies in the current technical infrastructure to appropriately audit any user's access to, creation of, modification of, destruction of, or transmission of personal health information. Because community health records and the creation of HIEs are relatively new, robust standards and related audit log technology have yet to be developed.

Many applications currently used in the health care industry for the transmission or processing of personal health information do not include adequate audit log capability, especially legacy applications (older applications built on what would be considered an outdated software platform). Several state teams raised concerns about the inability within their own applications to track external entities that may have accessed personal health information stored in proprietary databases and in EHRs.

Moreover, some state teams indicated that, once again, a lack of trust exists between organizations where one organization perceives adequate audit processes have not been implemented. Adequate audit processes mean more than activating the appropriate audit logs; they include the development and regularly scheduled use of an appropriate audit program that addresses potential security risks and privacy risks and is based on an established set of audit criteria that match the organization.

Suggested solutions to auditing issues include: the creation of guidelines for audit control and proactive monitoring; the use of a time/date stamp when a record is accessed, created, modified, destroyed, or transmitted; periodic tests of system controls that protect against breaches, virus, or spyware infection; and audit capability for e-mail and other methods of transmitting personal health information. A few states mentioned that if stringent audit requirements were imposed, additional support staff would need to be hired to maintain, monitor, and analyze the large quantities of data captured by the audit process. Many small providers may not have the funding to hire additional staff, resulting in a barrier to implementation. Although minimum audit requirements are needed to ensure the privacy and security of the data and are required by the HIPAA Security Rule, the cost issue must be taken into consideration when determining the appropriate level of audit requirements. The creation of cost-effective, efficient, and automated proactive mechanisms to assist with audit control could help with this issue.

As part of its overall implementation plan, one state plans to review the technological standards and operational policies and procedures set forth for nationwide health information exchange to ensure that they provide adequate guidance to the state about cost-effective and efficient automated proactive audit mechanisms. Other states plan to work with members of the health care community and security professionals to implement consensus model documents for EHR topics, including audit policies and procedures.

6.4.2 Secure Transmission of Data

As providers migrate from a paper-based to an electronic system, security data transmitted from electronic health records becomes an ever-increasing concern. The HIPAA Security Rule requires that a covered entity implement procedures to prevent unauthorized access to *protected health information* that is being transmitted (45 C.F.R. § 164.312(e)). However, no specific guidance is provided in the regulation about how to achieve this protection against the interception of electronically transmitted data.

In addition to *protected health information under the HIPAA rules*, a special category of data is designated as *specially protected health information* under other federal regulations and state laws, which includes information relating to alcohol and substance abuse, mental health information, sexually transmitted diseases, and HIV/AIDS status. At the federal level, alcohol and substance abuse treatment information is governed by 42 C.F.R. pt. 2. Additionally, many states have laws that similarly govern the exchange of *specially protected health information*, although the definition of *specially protected health information* may vary from state to state. Currently, because state and federal laws require additional permissions or other considerations when one is transmitting specially protected data, many states simply do not send any information associated with these categories of information. One solution was related to amending both state laws regarding *specially*

protected health information and 42 C.F.R. pt. 2 to allow for the freer use of secondary data and for the release of this information for treatment purposes without *consent*.

State teams raised the issue of segmenting of *specially protected health information* during transmission. Although 17 states included a discussion on *specially protected health information* in their solutions reports, only 6 discussed technical solutions for integrating this data into electronic health information exchange systems. One solution was to require opt-in/opt-out procedures for patients and methods for capturing and transmitting that information within and between systems. Technology-based solutions to segmenting the data included the use of filters to suppress data access to end users, increasing layers of computer security, using flags within databases to identify *specially protected health information*, and notifying end users that some *specially protected health information* has been blocked. However, technology solutions tend to require extensive planning, programming, and the potential to increase the workflow burden on the provider.

The state teams identified broad variation in practices associated with the exchange of personal health information, including variation in data definitions and transmission protocols. Definitions of key data elements describing procedures, treatments, and patient characteristics are inconsistent across entities, compromising the comparability of health information maintained by different providers. Reports cited stakeholder issues, such as the lack of interoperable solutions and the high cost of implementing appropriate forms of security that protect the data during transmission. State teams reported a lack of understanding about technology that is currently available and the cost of such solutions.

Currently, to exchange information and ensure transmission is HIPAA Security Rule compliant, many state teams indicated that entities rely on BAAs with other entities with which they would like to exchange data. This is also true for many RHIO settings and although it is widely assumed that all partner organizations in the RHIO must maintain minimum security requirements, there is always a concern that a participant with weak security measures could compromise the security of all participants.

Seven state teams noted that the standardization of BAAs and other types of agreements may help reduce or eliminate major obstacles to data sharing. Although the construction of model or standardized agreements is largely an issue of creating consensus around policies, these policies must include specific indications of *minimum necessary* technology requirements. Supplemental provisions in BAAs may be used to define standards for data confidentiality and integrity during end-to-end electronic exchanges, and also serve to outline parameters for the interoperable mechanisms used to uniquely identify patients and health care providers between systems. Where BAAs are not required, such as for most exchanges between providers, health care plans, and health care clearinghouses, the same kind of provisions may be implemented through other kinds of agreements.

State teams also raised the issue of standardization of data transmission requirements. While the technology exists to ensure the private and secure transmission of data, too often organizations do not communicate about standards for electronic transmission or available technical solutions to assist with secure data exchange. Seven of the state teams offered specific technical solutions to encourage electronic health information exchange. Solutions for secure transmission included the development of standard policies and procedures for the encryption and transmission of electronic data, including the development of a single set of regulations governing the parameters for electronic health information exchange, clarifying rules governing the use of electronic signatures, the use of public key infrastructure (PKI), and the development of a secure web portal for health data exchange. Solutions for secure electronic messaging between entities include enforcing encryption when e-mailing personally identifying information, adoption of scalable technology to accommodate secure transmission of data, and the creation of a consensus framework for a shared secured messaging platform, including technical and functional requirements.

Several state teams plan to draft suggested language to amend current state and federal laws governing the transmission and exchange of *specially protected health information*. Other state teams saw this as an opportunity to work with neighboring states to standardize policies and procedures on sensitive health information. Several state teams plan to recruit subject matter experts to work with committees or work groups to set and implement standards for the transmission of personal health information. State teams would have to find sponsors to oversee the initial effort to form these committees. For the steps in one state team's implementation plan, the subject matter expert would participate on a voluntary basis with little support from the sponsor. These committees would need to create agendas and timelines for developing the standards, including critical milestones.

6.5 State Laws and Interstate Issues

Most of the variation discussed (up to this point) has occurred because of varying applications and interpretations of the HIPAA Privacy and Security Rules, or the myriad factors that organizations must consider when constructing policies governing patient permission. Another major source of variation in business practices and policies stems from each state's unique privacy and security laws. Some of these issues have roots in federal legislation, although the true source of variation often lies in the state statutes. A major reported source of variation, state law that applies to sensitive health information, is discussed in Section 6.2.4, which addresses the variance in patient permission requirements. Other major issues reported as driving the variation in state laws are discussed below.

6.5.1 General Issues in State Law

Many proposed changes to state law are very specific and apply to narrow circumstances in a single state. For example, one state has a law that requires extensive documentation of

disclosures of information, even verbal communications among medical staff treating a patient in a single facility. Locating these laws and determining potential solutions requires a thorough legal analysis. State teams have carefully considered the implications of amending state laws and, in many instances, have created options for language that could be used to amend the relevant law, and have discussed the pros and cons of each choice, and the implications of leaving the law as is. These narrow changes are not addressed in detail here, but following is a list of general areas where state teams hoped to amend state law.

- Update or create legal definitions of terms (ie, *medical record* or *record locator service*) to apply to electronic exchange.
- Amend state privacy laws that do not apply to electronic exchange to include protections for electronic data.
- Create enforcement mechanisms for any new privacy or security laws.
- Consolidate state law or compile a compendium of relevant state law, federal law, and case law to facilitate legal analyses.

State teams were careful to note that they wished to proceed cautiously in amending state law, observing that there could be unintended consequences of the change, such as inadvertently limiting exchange instead of facilitating it. State teams also noted that they would have to examine the implications of mandating any sort of standards, pay special attention to providers that may lack the resources to adopt new technology or standards, and consider the impact on a wide range of stakeholders.

6.5.2 Public Health and Emergency Response

Many state teams reported uncovering significant challenges because of variations in the way public health entities undertake interstate communications for electronic health information exchange. The variations occurred largely because of the differences in state law governing reporting, differences in privacy and protection of health information, and disparate business practices.

One state team noted that stakeholders were not entirely sure whom to notify in other states in the event of a public health or other emergency, or how to notify them outside of business hours. One state indicated that a national law is needed that standardizes the process for handling people with communicable diseases who intentionally put the public at risk when they cross state lines. Additionally, an agreement about patients with diseases requiring cross-border information sharing would be helpful, as would standardizing the means by which personal health information is transmitted from one jurisdiction to another. Currently, the response to a communicable disease varied depending on the magnitude of the risk on public health, including whether the infected patient planned to travel by airplane and the type of disease. Other work, such as the creation of a uniform patient permission for or model law to govern interstate exchange, could easily encompass the issues of emergency communication.

Others noted that public and state officials expressed concern about the lack of integration in their systems. They felt that public health remained compromised because of the inability of systems to easily track and monitor threats to public health. State teams generally agreed that significant technological barriers to adopting more integrated electronic systems existed among physician groups or clinicians, hospitals, county health departments, and other organizations. To identify how they might exchange information more easily, several state teams planned outreach efforts to other state agencies that needed personal health information under certain circumstances.

Many state teams suggested that the ability to verify facts and transmit to or coordinate with other states would be greatly enhanced by an interoperable, electronic clinical information system or registry. On the other hand, at least one state team mentioned that its stakeholders felt that personal relationships are often a key element in transmitting data in a public health emergency, and an electronic system might remove the important human element.

A common theme in the state team reports was that state law and regulations were not sufficient to ensure private and secure electronic health information exchange with other stakeholders, such as law enforcement. Stakeholders must be assured that public health officials will participate in local and state planning for homeland security measures. Providers and public health agencies need to work with law enforcement and other organizations involved with bioterrorism to establish new standards and definitions about what personal health information is appropriate to disclose, when disclosure is appropriate, and for what purpose. Several states also suggested that the OCR decision tool could help remove many national barriers, including privacy and security barriers. This web-based interactive decision tool, they noted, was designed to help emergency preparedness and recovery planners better prepare for man-made and natural disasters. A particularly significant observation noted by state teams with experience in actual events (or trainings for them) addressed the need for hospitals to implement procedures for informing family members of missing relatives brought to the hospital.

One scenario revealed a clear chasm between the medical community and law enforcement, which severely restricted the exchange of information and impacted the delivery of health care. Law enforcement personnel reported that they try to obtain as much information as possible before a person enters a medical facility, a process that causes delay in transporting the person to a hospital. They viewed this delay as a necessary operating procedure because of increased difficulties in obtaining and collecting information once a person enters a medical facility. Several state teams noted how providers and law enforcement officers' lack of understanding of each others' differing roles could impact the treatment of the person detained.

At the state level, state teams planned to offer training for law enforcement and public health officials to educate them about what is required to exchange personal health information, that is, how to comply with state and federal law. One state has already incorporated training into their service academy curriculum.

6.5.3 Medicaid

Nearly all state teams mentioned Medicaid confidentiality standards as a barrier to electronic health information exchange. Both federal and state laws require that disclosure or use of Medicaid data concerning applicants or recipients must be limited to "purposes directly concerned with administration of the plan."[15] Medicaid plan administration is narrowly defined and only includes determining eligibility and amount of assistance, providing services to recipients, and conducting or assisting with investigations, prosecutions, and civil and criminal proceedings related to administration.[16] In addition, information concerning Medicaid applicants or recipients may be shared only with persons who are subject to standards of confidentiality that are comparable to the Medicaid confidentiality standards. These restrictions apply to all requests for information from outside sources, including other governmental bodies.

Interpretation of what activities are directly concerned with "administration of the plan" varies widely from state to state. For example, one state reported that although it has a state registry of childhood immunizations that operates as a public authority under a contract with the state, Medicaid does not share immunization data with the registry, creating an incomplete picture of immunization rates among low-income children. One state tried to negotiate a memorandum of understanding (MOU) between the registry and Medicaid to remedy this situation. Another state is currently pursuing exchange with the state Medicaid program but has encountered major problems with sharing data. Yet another state, reported, however, that it has already successfully addressed the issue of access to Medicaid data. They noted that Medicaid generally allows data sharing with Data Use Agreements when the study seeks to improve the administration of the State Medicaid Plan. They noted that their health department already collects and maintains immunization and lead data through statutory authority or legal agreements, with processes in place to maintain confidentiality of the data.

---

[15] Each state administers its own Medicaid program, while the federal Centers for Medicare & Medicaid Services (CMS) monitors the state-run programs and establishes requirements for service delivery, quality, funding, and eligibility standards. With respect to confidentiality, the federal statute and regulations require that state Medicaid programs implement safeguards to protect Medicaid data. Thus, state standards actually restrict exchange, although federal statute and regulations mandate those standards.

[16] The federal law can be found in the Social Security Act (42 U.S.C. §§ 1396a(a)(7), 1902(a)(7)). The regulations can be found in 42 C.F.R. § 431.300 *et seq.* The definition of plan administration is found in § 431.302.

Although several states proposed legislation to govern the exchange of information between these entities, other states felt that the federal government should recommend a solution to resolve this issue. In fact, several years ago CMS (then known as the Health Care Financing Administration) issued a Medicaid Directors Letter intended to clarify circumstances when sharing of Medicaid data was appropriate. This letter gave several examples of cooperative data sharing between Medicaid and public health agencies considered to benefit the administration of the Medicaid Program, including

- improving the technical capacity of states to analyze data from multiple sources to support policy decision making and program monitoring;
- promoting the development and implementation of common performance measures across multiple programs to improve their effectiveness; and
- using Medicaid encounter data more effectively to assist in public health surveillance to ensure appropriate care for the Medicaid population.[17]

Although the position taken in this letter has never been formally revoked, neither has it been reaffirmed. The most recent Medicaid Directors Letter on the privacy and security of Medicaid data reiterates that "use or disclosure of information concerning applicants and recipients is permitted only when directly connected to administration of the State plan," and appears cautionary in tone.[18] Clarification by CMS whether it still endorses its prior position that cooperative data sharing between Medicaid and public health agencies can, in appropriate circumstances, be considered to directly relate to the administration of the Medicaid Program may help alleviate some of the state variance on this issue and foster appropriate electronic health information exchange.

6.5.4 Licensing

The issue of variation in licensing was mentioned infrequently, although differing legal definitions used in licensing health professionals complicates the examination of interstate personal health information sharing. One state team proposed linking licensing to provider digital identity services to facilitate authentication of providers.

6.5.5 Interstate Exchange

State teams are still in the preliminary stages of exploring interstate exchange. They clearly recognize the need for interstate communication and clarification of cross-jurisdictional legal issues, but have focused their energy on building infrastructure in-state first. The issue of interstate exchange is especially pressing in areas with large cross-border markets and in states with large numbers of tourists, college students, seasonal workers, or other temporary populations. Interstate exchange also applies to disaster planning. A number of

[17] Health Care Financing Administration letter to State Medicaid Directors, "Facilitating Collaborations for Data Sharing between State Medicaid and Health Agencies," (October 22, 1998), available at: http://www.cms.hhs.gov/SMDL/SMD/list.asp.

[18] CMS letter to State Medicaid Directors, "Privacy of Medicaid Data Records," (September 20, 2006), available at http://www.cms.hhs.gov/SMDL/SMD/list.asp.

issues must be addressed for successful interstate exchange to occur, including how patient permission would be handled, how sensitive information would be handled, and what state would have jurisdiction if an issue arose as the result of an interstate exchange.

As discussed in Section 6.2, states take a variety of approaches to patient permission. Some have state laws do not require permission for treatment, while others require patient permission for each disclosure. States with more stringent laws expressed concern that information would not be treated with their required level of protection if it were shared with a state less strict standards. As also discussed in Section 6.2, states often have varying requirements for patient permission for the release of sensitive information, and the definition of *sensitive information* varies between states. States will need to resolve these discrepancies to successfully engage in interstate exchange.

State teams mentioned a number of strategies for collaborating with both regional partners and states across the country. A number of states proposed collaborating with the National Conference of Commissioners on Uniform State Law to create a model law to apply to interstate exchange. Other options included establishing an interstate task force to develop HIE procedures and review the laws relevant to exchange between states or implementing compacts or an MOU to allow interstate exchange. Some states have already begun reaching out to their neighbors. Their successes may serve as a model for states that have not yet begun outreach.

6.6 Trust in Security

Many of the state reports raised the issue of trust as critical, specifically in the way it affects the potential adoption and viability of electronic health information exchange. Throughout the majority of state reports, 2 major groups of stakeholders expressed concerns with electronic health information exchange: consumers and providers. Consumer concerns tended to focus on privacy risks from the implementation of new technologies and the potential for unauthorized disclosures of sensitive information to payers and employers. Providers were principally concerned about potential liabilities from the activities of other participants in electronic health information exchange and about consumers' lawsuits for inappropriate disclosures of their information; they were secondarily concerned about potential uses of patient information by payers, law enforcement, and public health officials. The latter concern had less to do with trust in the security of the EHRs themselves and more to do with how these systems might manage the competing interests between groups about access to EHR data.

The review of trust issues was complicated by the fact that critical issues and business practices data were not typically categorized under this heading, although trust emerged as a major underlying factor. In some cases trust (or lack of it) seems to have been a motivating reason for the variance in business practices. In a number of cases, stakeholder

groups (other than consumers) articulated their impression that consumer lack of trust was a critical issue, but there was little or consumer input to support or deny the concerns. Ten reports lacked information that either expressly or by reasonable inference raised trust as a critical issue.

6.6.1 Providers

Providers' mistrust of electronic health information exchange is related largely to their concern about no having control over their patient's information once it leaves their offices and the potential this lack of control may open up for lawsuits and liabilities for wrongful disclosure. This issue was identified by 10 reports and was based, in most cases, on the fear of liability for errors or improper actions by other parties participating in an HIE. One state identified this fear as their single most significant issue, one which had been repeatedly raised, and the reason providers were not willing to participate in electronic health information exchange. State reports seemed largely unable to uncover specific experiences that provide the basis for this fear. One team identified a specific statute giving patients a cause of action for inappropriate disclosure, and another reported that HIPAA-based claims were included in lawsuits by patients frequently: one provider had reported 6 such claims within the preceding 6 months. However, a Bureau of National Affairs (BNA) Health Care Policy Report summarized the results of nearly 500 judicial opinions to determine whether HIPAA acts as a legal barrier to electronic health information exchange because of interaction with more stringent state laws. The findings indicated that "none of the decided cases involve the denial of access to providers who seek personal health information for the purposes of treatment, quality improvement or the production of transparent information." (BNA, 2007). Most commonly, the cases dealt with a health care provider trying to use HIPAA as a shield to defend against litigation, but there was no evidence that either HIPAA or any of the more stringent state laws would ever preclude the transfer of essential information at the point of treatment.

Although no legal basis exists for the fear of liability for a disclosure made for treatment purposes, the fear clearly exists and is a barrier to otherwise appropriate electronic health information exchange. A review of these issues, as discussed in the individual state reports, also indicated that providers' lack of trust (that disclosures in an electronic system would be compliant and not yield liability) appear to be directly correlated with electronic health information exchange experience. In other words, providers in states with relatively few electronic health information exchange activities, or a briefer history of such activities, appear to fear they may be held liable or penalized for engaging in them and, in some cases, do not trust the technologies. Providers in states with more experience do not appear to have such concerns, or have them to a lesser degree.

6.6.2 Solutions and Implementation Plans

A significant issue underlying the lack of provider trust in electronic health information exchange is the general lack of understanding or knowledge of existing functional requirements and standards. One solution for increasing the knowledge base for electronic health information exchange within all stakeholder groups, including providers, is the creation of a body to provide centralized health information exchange and HIT organization. Whether this group is a centralized authority, as proposed by 8 states, or just a coordinated effort to increase stakeholder involvement in electronic health information exchange, as proposed by 10 states, the outcome would likely be the same: enhancing the adoption of electronic health information exchange and providing increased privacy and security safeguards.

Although the exact makeup of these governance structures or committees varied slightly, they were commonly tasked with identifying standards, defining protocols, conducting pilot projects, or offering training. They could also compile best practices and disseminate them to stakeholders such as providers. State teams clearly felt the need for common vocabulary and data standards if interoperability is to be achieved. To ensure coordination among these different efforts in the states, it would be important to dovetail with the work of HITSP, discussed further in Section 7.

States found that many health care professionals did not have an accurate or complete understanding of HIPAA regulations or relevant state laws. States reported that educating and training providers was essential, especially on state and federal privacy and security laws and regulations and the types and benefits of electronic health information exchange systems. Additionally, states suggested providing continuing education for all professional health care staff in organizations that use an electronic health information exchange system to ensure proper privacy and security procedures are followed.

According to the American Medical Association, the top 3 concerns among providers who have not adopted HIT are the cost of adoption of new technologies, uncertain return on investment following implementation, and worries regarding obsolescence. In addition to financial considerations, physicians are also concerned about the privacy and security of patient data, HIPAA compliance, and the potential for inappropriate disclosure of personal health information.

To address provider concerns, state teams proposed training programs, possibly offering continuing education units. State teams are aware that past educational efforts for providers on privacy and security have had limited success, especially those on HIPAA, and are determined to adapt and learn.

6.6.3 Consumer Trust

Another significant trust issue was consumer lack of trust, which appeared to have been expressed directly by consumers in 4 reports and was an issue perceived by nonconsumer participants in 6 others. The principal basis articulated for this lack of trust was concern about payer and employer access and, secondarily, distrust of new technologies. One major reason for this lack of trust was the substantial number of security breaches that were reported over the last few years, including several involving health care organizations. A recent survey by the Kaiser Foundation found that while 72% of respondents believed the electronic records were more efficient, nearly half also felt that paper records were more secure (Conn, 2007). However, the same study also found that, prior to participating in the survey, 57% of respondents had not seen, read, or heard anything about EHRs, which indicates a fundamental information gap about electronic health information exchange within the general consumer population.

A secondary issue underlying both issues of access to the data and risk of breach involves the type of information that would be stored and transmitted as part of an electronic system. Namely, the majority of patients may not be concerned if a data breach released information regarding a simple visit for seasonal allergies, for example, but they would be concerned if that breach included information regarding treatment for a sexually transmitted disease. Discussed in detail in Section 6.2.4, the special data security requirements for *specially protected health information* (which vary from state to state, but typically include HIV/AIDS, mental health, substance abuse treatment, and genetic testing) are a major focus of those working on an electronic health information exchange infrastructure. Relaying this information to consumers and ensuring that they are comfortable with the data security decisions regarding all of their health information, including information that they feel should be specially protected, is an essential consideration to electronic health information exchange efforts moving forward.

6.6.4 Solutions and Implementation Plans

Many consumers lack knowledge of their existing health information privacy rights, as well as current security obligations and practices of health care organizations. Consumers not only need to be educated about their rights, but also need to understand who can access their information. This lack of knowledge is likely to create a significant trust issue as electronic health information exchange is implemented, since privacy and security rights and obligations are not yet well defined for electronic health information exchange.

Education programs could not only be used to increase consumers' involvement in the management of their own health data, but also to inform them about their rights, advantages of EHRs, patient permission issues, and recent developments in technology and security. Many states recommended leveraging existing consumer education venues such as doctor's offices, clinics, and established websites, hosting focus groups, creating educational

packages, and producing frequently asked questions documents as ways of educating the public.

Another suggested solution calls for the establishment of a centralized method to develop and distribute educational materials concerning patient rights and responsibilities, as well as enabling consumers to protect and monitor their own health care information. Educational materials should include information regarding the technology used in an HIE to help consumers understand the technology and their ability to interact with it.

These education and outreach solutions were important components of most implementation plans. Many times, educational components were built into other initiatives, such as standards development or changes to state law, while other state teams proposed separate plans to educate stakeholders, including consumers.

State teams proposed educational campaigns to increase awareness of the benefits of EHRs and electronic health information exchange, and also educate them about their rights and responsibilities. States recognized the need for consumer engagement and education, noting that buy-in was critical to the success of electronic health information exchange. States planned general educational campaigns, noting that they had yet to identify the best media for disseminating their message or had not yet determined what sort of content to include. Many of the states will need to do additional research in order to craft and transmit their messages. At least 2 state teams felt strongly that creation of a consistent message among states was also needed to ensure a proper foundation for nationwide electronic health information exchange activities.

Although primarily a technology issue, the segmenting of specially protected data is a component of trust that may become more important to consumers as electronic health information exchange continues to grow and expand. As discussed earlier in the report, many providers simply do not exchange information that is specially protected, because of the additional patient permissions, or other considerations necessary to appropriately transmit the data. At least 1 state suggested opt-in/opt-out procedures for patients and methods for capturing and transmitting that information within and between systems.

Involving patients more directly in their own health care decisions is technically feasible and it could engender consumer trust of electronic health information exchange systems, but it also exposes a tension between consumers and other stakeholders. Allowing patients to direct where and how much of their health record data are sent draws patients into the health care process, eases the creation of personal health records and their associated applications, and permits individual flexibility related to privacy. More importantly, it also returns the issue of who is included in the information flow for a patient's care to a dialogue between patients and their health care provider. Individual consumer involvement in the health care information exchange may result in an increased awareness of privacy and security issues in the general population. Although this model addresses many current

issues related to electronic health information exchange, it raises other issues that are just as complex. For instance, what happens if patients block access to data that could potentially save their lives? And, how do you involve those that do not have access to computers or do not understand the complexity of issues that must be considered when making these decisions? Resources, such as the guidelines for personal health records described by the Markle Foundation's Connecting for Health report and person-centered RHIOs such as the Louisville Health Information Exchange (LOUHIE), can be utilized when considering these issues.

6.6.5 Trust Within Other Stakeholder Groups

Although education of health care providers and the general public dominated states' educational solutions, some important education-based solutions were proposed for special groups of stakeholders. Special considerations needed for these groups were often uncovered in the assessment of variations process when a general disconnect existed between certain stakeholder groups that were either forgotten in discussions involving electronic health information exchange, or groups that had particular interest in a more controversial aspect of electronic health information exchange.

States suggested creating targeted education and outreach materials to these groups. Specific solutions include conducting joint training events for law enforcement and public health, target training/educational programs for law enforcement and public officials (including judges) to explain HIPAA Privacy and Security requirements, and education of HMOs and employer groups on the benefits and use of data for research purposes. Engagement with law enforcement is particularly important in rural areas, where police officers are frequently the first responders to an accident and assist in patient care. Collaboration with public health offers opportunities for improved disease surveillance.

6.7 Standards for Patient Identification

A variety of states noted that definitions of key data elements describing patient characteristics were inconsistent across entities, compromising the integrity of health information maintained by different providers. One of the most promising factors of electronic health information exchange is the possibility of more complete and accurate matching of patient data from provider to provider.

Patient and provider identification across organizations is required to

- improve administrative efficiencies and reduce health care costs by minimizing the collection of redundant information and by reducing or eliminating the need to perform redundant tests (because of the inability to access information about a patient in a timely fashion);
- provide better-quality care, avoid medical errors, and improve patient safety;
- control against identity theft, fraud, and abuse;

- appropriately match data about an individual from one organization to another when health information exchanges are performed;
- appropriately authenticate a patient or a provider to come into an organization's system;
- establish access controls to certain health information on the basis of the authenticated identity of a patient or a provider;
- implement mechanisms to prevent inappropriate access to data or monitor the access to data by patients and providers; and
- implement core electronic health information exchange functionality.

Recent developments in the area of personal health records have also advanced the need to establish a consistent and reliable method for linking patients to their records so that authorized providers and other users can locate the right information about the right patient.

6.7.1 Types of Patient Identification Used

Current practices reported by participating stakeholders from most states indicated the use by organizations of unique, asynchronous, and incompatible methods to establish the identities of their patients, enrollees, clients, and consumers. State teams reported instances, even within organizations, in which the same patient had been assigned more than one ID (eg, a patient's ambulatory or primary care clinic record vis-à-vis the same patient's inpatient or hospital record). Although this multiple assignment of ID is often caused by errors such as spelling variations in names and transpositions of dates, some hospitals intentionally assign a different identification number to the same patient for each admission.

According to states, verification of patient identification across different systems can be an even greater challenge. Currently, each organization—hospital, clinic, physician office, or RHIO—employs their own algorithm and patient matching methods, resulting in inconsistent patient matching. Although various algorithms currently used provide a relatively high level of matching (given a few piece of personal information), no algorithm-based system is perfect. Thus, <u>all</u> relevant information for a particular patient may not be identified. The reverse situation, where more than one individual's health information is contained in one record, is commonplace, especially in states in which large numbers of uninsured and possibly illegal aliens reside. Compounding the problem is the prohibition of using Social Security numbers in medical records in certain states, making patient matching even more difficult.

6.7.2 Different Identification Systems: Common Challenges

States highlighted the following challenges associated with the variability and incompatibility of patient identification systems and approaches. These included

- inability to appropriately link patient information across systems for delivery purposes (applicable to both paper and electronic environments);
- inability to create longitudinal, multifacility continuum-of-care episodes for a patient;
- inability to track patients across a full episode of care and monitor performance of the health care system; and
- the lack of interoperability across systems for purposes of identifying providers, which forces a patient's providers to "jump" from one system to the next to gather and manually integrate all the information available on him or her instead of using automated methods to aggregate the information across sources.

Provider-related challenges included the need to access health information about a patient (residing in different systems) and the need to know all the unique identifiers assigned by those systems to the patient to access the information accurately and reliably.

The ability for a health care provider to identify the correct records for a patient is critical to clinical medicine and to health information exchange. The lack of a standard, reliable way of accurately matching records to patients introduces the potential for inappropriate use or disclosure of personal health information about the wrong patient, which is both a clinical and a privacy risk. This risk is particularly acute when information is shared across institutions that use different methods of patient and record identification.

Many state teams reported 2 other major challenges: the variability in methods across organizations to link patients to records, and the lack of agreed-upon patient-to-record matching standards to apply when interorganizational electronic health information exchange is conducted. These challenges did not exist in uniquely identifying *providers* across the health care system, because new federal HIPAA regulations have now established a national standard unique identifier for health care providers, the National Provider Identifier (NPI). Providers, payers, and others were required to fully implement the NPI by May 23, 2007.

Given the lack of a national (or state) unique patient identifier, state teams discussed several alternatives for future use under organized regional networks and aimed at addressing the need for matching patients to their records across systems. One frequently cited mechanism was the so-called record locator service (RLS), a centrally administered functionality of a health information network that provides the requester of data with the location of data about a specific patient. The RLS uses various identifying characteristics of individuals to create a match and point to the location of health information about that individual.

Other mechanisms considered varied from the creation of a regional Master Patient Index (MPI), to using exact or deterministic record linkage approaches, to more sophisticated record linkage methods employing advanced statistical algorithms and probabilistic record matching formulas to establish a true match and minimize false-positives.

6.7.3 Solutions and Implementation Plans

The ability to accurately identify patients across systems was an issue in many of the states, with 16 state teams suggesting technical solutions to this issue. For the most part, these state teams agreed that some system of identifying patients between entities must exist for true interoperability to occur, and that these systems must include stringent matching criteria to ensure that patient records remain confidential.

As enacted by Congress, HIPAA (the act) provided for the creation of national unique patient identifiers; however, HHS and Congress have put the development of such a standard on hold indefinitely. In 1998, HHS delayed any work on this standard until after comprehensive privacy protections were in place. Since 1999, Congress has adopted appropriations language to ensure no appropriated funds are used to promulgate such a standard. States have considered a number of alternative technical solutions, such as better matching algorithms, to improve identification of patients.

State teams suggested creating standards for matching that included minimum, as well as optional, data elements. Specific solutions included establishing biometrics as the preferred method of verifying the identity of patients, creating model policies and procedures to ensure appropriate capture of patient identifiers, and developing an MPI with patient identification algorithms to facilitate accurate exchange of information. Many examples of successful MPI programs exist, and these types of systems are officially endorsed by leading policy groups such as the Markle Foundation's Connecting for Health project. Although early attempts at such programs raised additional concerns regarding improper matching and inappropriate disclosure of records if multiple matches were found, in systems that have already been developed, nearly 100% of records matched (Brewin and Ferris, 2005).

Identifying providers is also an issue in electronic health information exchange, and is linked to authorization and authentication. States and electronic health information exchange participants need a system that ensures they are providing information to individuals who legitimately require access to the data, and that they are who they claim to be. HIPAA requires the adoption of a standard unique identifier for health care providers. The NPI number must be used by all HIPAA *covered entities* as of May 23, 2007 (small health plans have until May 23, 2008, to comply). The NPI is a 10-digit "intelligence free" identifier. That is, it does not carry any personalized information about the provider. Guidance from HHS and CMS notes that having an NPI "does not ensure that a provider is licensed or credentialed." State teams proposed creating state-level provider registries that would also include authentication and authorization processes. These state-level registries could potentially link to the NPI.

6.8 Cultural and Business Issues

State teams referenced cultural and business issues that pose challenges to electronic health information exchange. One example is concern about liability for incidental or inappropriate disclosures, which causes many stakeholder organizations to take a conservative approach to developing practice and policy. This concern is discussed in greater detail in Section 6.3.6. General resistance to change is another business issue that organizations face whenever a change occurs in how business is conducted, which in turn, can cause workflow modifications. Such resistance is frequently cited as a cultural issue in discussions about decisions to adopt electronic systems. Some individuals within organizations are comfortable with existing paper-based or manual systems and data exchange practices and processes, and they believe that current manual practices produce accurate data and are timely and effective. Implicit in some discussions is an assumption that security slows down the process: the data are secure but are not transmitted as fast as they can be with a quick phone call. In fact, most data exchanges take place via person-to-person contact, especially in emergency situations, and human judgment plays a large role in how and when information is exchanged. It will be critical to include these points at which human judgment is required in the specifications for any system developed to exchange information. Moving toward interoperable health information exchange requires awareness of the human elements of health information exchange, as well as an understanding of how to alleviate concerns, such as those surrounding the adoption of EHRs.

6.8.1 EHR Adoption Issues

Resistance to the adoption of EHRs is often driven by the cost of implementing EHRs and the uncertainty of the return on investment. Implementing EHRs requires a substantial investment, and many smaller provider groups, safety net hospitals, or other providers that serve low-income populations may lack the capital needed for such an investment. In addition, the process of implementing EHRs is challenging and requires significant attention to detail to train workers, adjust workflows, and ensure that the quality of care is maintained. To address this issue, state teams planned to implement support programs for providers, such as educational cooperatives and financial incentives, to encourage EHR adoption. State teams also planned pilot projects to demonstrate the return on investment. Determining the value of EHR adoption and interoperability may help providers overcome their financial concerns, and education may alleviate other worries.

State project teams also indicated that sample material explaining the benefits of health information exchange and the sharing of data for treatment purposes and to improve the quality of care would be useful for encouraging adoption of HIT. It would be efficient for some material to be developed, and to share these sample materials broadly. Of course, these materials may need to be tailored to the specific state law situation; however, using the material as a starting point would likely be helpful to states.

In addition to the cost of implementing EHRs, some providers are wary of violating the Stark physician self-referral (Stark) and health care anti-kickback laws. The laws have been repeatedly identified as potential barriers to the donation of applications and services. The state teams were largely unaware of action taken in 2006 by HHS when it announced new regulations allowing exceptions for certain arrangements in which (1) a physician receives compensation in the form of items or services (not including cash or cash equivalents) that are necessary and used solely to receive and transmit electronic prescription information; and (2) involving the provision of nonmonetary remuneration in the form of electronic health records software or information technology and training services necessary and used predominantly to create, maintain, transmit, or receive electronic health records to facilitate adoption of EHRs.

6.8.2 Business Practices and Terminology

Another business issue that cuts across all the scenarios and domains is the need for clear definitions of terms within state and federal laws. For example, terms like *medical emergency*, *current treatment*, *related entity*, and *minimum necessary* do not have agreed-upon definitions and, therefore, increase variation as organizations attempt to meet compliance by defining terms in ways that protect the interests of the organization. The term *health record* is a good example: organizations disagree about whether or not a patient's demographic data and a pointer to the location of a patient's health information constitute a *health record*. These terms may need to be defined in state or federal law. Model laws could also help resolve the inconsistencies in interpretations and applications and facilitate exchange across state lines.

Another example of a cultural and business issue involves the tension among health care providers, hospitals, and patients concerning who controls or owns the data (see Section 6.3.5 for additional discussion of information ownership). A number of providers indicated that they did not think that patients should have full access to their records, especially to doctors' notes even though the HIPAA Privacy Rule generally provides patients the right to access all of their *protected health information* in a designated record set. There was a concern that providers would not enter complete notes, as well as concerns about liability. However, the majority of stakeholders agreed that, to be successful, electronic health information exchange must be designed to address patients' needs, interests, and concerns.

In addition, state teams observed that widespread adoption and interoperability will not be achieved unless the human interface with health IT receives significant attention. Professional staff provide the information and control the flow of information through HIE systems, and their knowledge, or lack thereof, of health information exchange, and the protection of privacy and security is critical to success. As a solution to the variations experienced in staff knowledge, expertise, and training, state teams recommended

establishing core competencies for staff education, to include not only privacy and security training, but also awareness of the technical issues relevant to their job responsibilities and electronic health information. State teams also planned to host focus groups or information sessions with influential stakeholders to inform them of the national, state, and local activities of electronic health information exchange to build support for state and local initiatives. Building support among consumers and stakeholders will facilitate interoperable health information exchange.

7. FUTURE DIRECTIONS AND RECOMMENDATIONS

The goals for this project have been achieved. State teams reached out to stakeholders; conducted the assessment of variation in business practices, policies, and state laws; developed feasible solutions; and developed plans to implement these solutions. Each state team established relationships among key stakeholders and developed a body of knowledge that will carry into the future. While the state teams differ in experience and in the sophistication of their approaches, all have made significant progress in understanding their current landscape with respect to privacy and security practices, policies, and state laws; they have each identified next steps toward developing consensus-driven approaches to implementing privacy policy and security practices that will create the framework necessary to protect personal health information as it moves from a paper to an electronic platform. Looking across the state teams' reports, one can easily identify the major areas that call for coordination and leadership. To reduce the variation in practice, policy, and law identified by the state teams to a manageable range that will permit widespread electronic health information exchange, state teams must work with one another and with existing federal initiatives as they move forward.

State teams have prioritized plans based on the needs dictated by their unique local environment for electronic health information exchange. For example, states in the beginning stages plan to establish a foundation by identifying appropriate leadership and governance, whereas more advanced states' plans focus on a specific issue, such as developing a *consent management process*. Throughout the course of this project, state teams have raised a broad range of issues and recommended many ways to resolve these issues. To reduce variation nationwide requires a coordinated effort that brings representatives from all 56 states and territories together to work collaboratively on the issues raised and to work out solutions that have broad application and are coordinated with other federal initiatives.

In addition to funding state implementation plans, we have begun a new phase in this contract at the direction of the US Department of Health and Human Services (HHS): to cluster state teams into collaborative work groups with other states and territories that were not part of this contract so as to focus on issues with multistate or regional relevance and broad applicability. The collaborative work groups will come together on a regular basis to share their progress and ensure maximum knowledge transfer. In this section we offer observations and recommendations that flow from the nationwide summary that, if implemented, will facilitate the future work of the state teams and multistate and regional teams moving forward.

7.1 Leadership and Coordination With Federal Initiatives

One gap that was identified during the course of this project was the general lack of knowledge stakeholders and state project teams have about the health information technology (HIT) and health information exchange (HIE) activities under way at the federal level. Although a number of states are on the "cutting edge," generally, at the state-level, knowledge of or participation in major health informatics activities is extremely low. The concern here is that the states without knowledge of federal initiatives will adopt solutions to privacy and security issues that are not aligned with other initiatives, creating more variation instead of less. The State Alliance for e-Health Health Information Protection Task Force (formed during the course of this project) is one forum where states can receive information on federal privacy and security initiatives and exchange information among themselves. Other recommendations may facilitate communication and collaboration between federal and state privacy and security initiatives.

Recommendations are as follows:

- **Recommendation 1.** If the American Health Information Community (AHIC) successor organization forms a Confidentiality, Privacy and Security (CPS) work group, one member from that work group should serve as a state liaison. The state liaison would be responsible for meeting with the leaders of the state-level privacy and security bodies and carrying their concerns forward to the CPS and ultimately to the AHIC successor.
- **Recommendation 2.** The AHIC successor should host its meetings in a different region of the country at least twice a year and invite state and local leaders to attend and have the opportunity to inform the AHIC successor of activities and needs at the state and regional level. This would serve to increase the visibility of the federal initiatives to stakeholders nationwide, creating a more unified initiative.
- **Recommendation 3.** As a relatively inexpensive method to disseminate information in a timely way, HHS should publish a monthly or bimonthly electronic privacy and security newsletter that highlights the progress of the various privacy and security initiatives that the state teams have under way and how such progress has advanced the nationwide vision.

There are many ways to coordinate regular formal communication between the federal privacy and security initiatives and the state and territorial initiatives. The goal is to create consistent, accurate communication resulting in a clear direction from the federal government to the states.

7.2 Incorporating Privacy and Security Policies and Practices Into Governance Models

In the state implementation plans, the most frequently cited need was for some kind of state or local coordinating body that would organize and monitor electronic health information exchange activity, in general, and issues related to privacy and security, in particular. State teams that are in the early stages of adopting and using electronic health

record (EHR) systems focused more on plans to develop an organizing body to align all HIT initiatives within their states, including the privacy and security work, whereas state teams on the cusp of having working HIEs focused more on what the governance structure of an HIE should look like and how the privacy and security policies and practices would fit into that structure.

Although the focus of this work was not HIE governance, many state teams reported that HIE governance is a problematic issue. *Governance* in an HIE context is sometimes used to refer to activities that provide strategic direction, interoperable technical standards, and common privacy and security practices to the various groups and organizations administering and engaged in electronic health information exchange.[19] Currently, there is no single accepted electronic health information exchange governance model, nor is there any settled set of governance functions. Nonetheless, 22 of the state teams reported that they were implementing or intended to develop some kind of formal governance body to oversee electronic health information exchange implementation; governance-related functions were cited, running a gamut from comprehensive, prescriptive electronic health information exchange guidance to relatively narrowly targeted, problem-specific initiatives (eg, standardization of laws, security and privacy standards development, and standardized education).

Given the diversity of HIE models and functions that already exist, an authoritative description of *HIE governance* would be a valuable contribution. Although only limited case studies may be available, related resources can help focus discussion. Generally, IT governance attempts to align IT-based processes with operational (business) strategies and needs, while identifying and managing IT-related risks. IT governance is a policy-based activity in which a central authority provides strategic direction and guidance that is implemented by administrative and operative personnel. From these concepts, a good initial working definition of *HIE governance* might be as follows: "the infrastructure and processes used to develop, implement, and enforce policies, procedures and practices, including those policies, procedures, and practices that are specifically related to privacy and security, enabling electronic health information exchange between organizations."

This definition of *HIE governance* includes policy development functions consistent with concepts already recognized. In particular, it is consistent with the Foundation of Research and Education (FORE) recommendations to HHS (January 12, 2007) for a policy oversight infrastructure that would rely on the AHIC (or its successor) and state public-private partnerships to provide strategic direction to HIE activities. In this context, AHIC (or its

[19] See, for example, FORE (2007, p. 4): "Each state should establish or designate a consolidated, public-private health transformation governance mechanism that includes at least health information exchange and quality/transparency. . . . A public-private governance mechanism is needed to bring together governmental, healthcare, employer, and consumer stakeholders to set direction and align actions."

successor) and the state bodies would be the policy adoption, development, and promulgation component. This arrangement would exist particularly because most privacy and security safeguards and risks are associated with administrative—as opposed to technical—practices and standards.

However, effective governance requires an infrastructure for policy implementation and enforcement, as well, and this requirement may be more problematic. Without a comprehensive health information infrastructure under unified authority such as a federal or state agency—a governance approach which is not recommended here, and which none of the states has recommended—implementation and enforcement must be the responsibility of the stakeholders who administer and operate the networks used for electronic health information exchange.

The policy implementation and enforcement level is where a more in-depth analysis of the factors affecting the success of interorganizational HIE governance could be valuable. Although it is not possible to fully specify these factors at this stage, 3 types of factors appear to have the greatest effect on HIE governance: The geography of health care markets, HIE maturity of the participants, and cultural factors affecting the acceptability of centralized governance.

Recommendations are as follows:

- **Recommendation 4.** HHS should work with states and interested national organizations to establish an HIE policy adoption, development, and promulgation governance infrastructure to provide for nationwide consistency in HIE privacy policies and business practices.
- **Recommendation 5.** HHS should work with interested national organizations and other stakeholders to identify, analyze, and publicize the factors that affect HIE governance body success.

The principal goal of these recommendations is to provide authoritative guidance for the development of appropriate governance bodies for the implementation of electronic health information exchange, consistent with national policies and standards yet in the context of diverse state, regional, and market realities.

The deliverables should include pragmatic, useable descriptions and analyses of the principal factors affecting HIE governance structures and how they impact decisions about privacy and security policy and practices.

7.3 Alignment of State and Federal Legal Environments

Existing federal and state laws and regulations affecting the privacy and security of electronic health information exchange may be accurately characterized as a “patchwork.” Changing this patchwork to a more consistent nationwide framework in a manner that preserves appropriate state authority will require an organized process. Such a process

must address issues related to both paper and electronic exchange of health information, given that full adoption of electronic health information exchange will occur over time.

7.3.1 Aligning State Health Privacy Laws

Although the scope of this project did not include comprehensive legal analyses of state privacy and security laws, the state teams did find that in many cases state privacy law is not well understood by organizations and much current law does not apply to electronic health information exchange. Their proposed solutions included revising laws and regulations. This development is simultaneously valuable and problematic. Its value is obvious: in states where this process is occurring, it laws and regulations that do not apply to electronic health information exchange will likely be eliminated or revised; new laws and regulations will be drafted that take into account the difference in the type of privacy risks that will be faced as we move from paper to electronic exchange. This development is problematic to the extent that the states develop inconsistent new and revised laws and regulations.[20]

The State Alliance for e-Health (State Alliance) has begun the process of examining potential solutions to address the variance in state health privacy laws. It is analyzing state health privacy statutes and has obtained input from some of the state teams. In addition, the State Alliance is investigating the potential for the promulgation of a uniform or model state health privacy law, particularly to address the issue of *consent* or *authorization*. The National Conference of Commissioners on Uniform State Laws (NCCUSL) recently (June 15, 2007) presented information on the process of developing model laws to the Health Information Protection Taskforce of the State Alliance. The project teams are being coordinated in their efforts by the current project, which ensures that the teams are in regular communication. The formation of the multistate and regional collaborative work groups will continue this effort.

To make legal and regulatory changes that are backed by genuine consensus, and that are well-drafted and appropriate to the practical realities of current and future health care operations, it will be necessary to involve at least the core professions concerned with these issues. The American Health Information Management Association (AHIMA), the Health Information Management Systems Society (HIMSS) and the Workgroup for Electronic Data Interchange (WEDI) have been valuable contributors in this field already, and efforts to obtain comparable support from the other professions concerned with health care legal and regulatory issues should also succeed. For lawyers, the principal national associations are the American Bar Association, through its Health Law Section, and the American Health

[20] For example, a state may adopt new genetic-information privacy protections to help reduce consumer objections to information exchange. If neighboring states do not adopt similar laws, organizations in the state with such protections may be reluctant to send protected information to the neighboring state, fearing potential liabilities. Moreover, this situation creates significant issues for multistate health care organizations.

Lawyers Association. For privacy professionals it is the International Association of Privacy Professionals; for security professionals it is the Information Systems Security Association, as well as the International Information Systems Security Certification Consortium. These professional groups in many ways already provide valuable support to the overall initiative and may be useful resources for state governments and state-level stakeholders working to resolve legal and regulatory obstacles at the multistate level.

7.3.2 Interpretation and Application of Federal Laws

One of the important findings across the state teams was that there is substantial variation in the interpretation and application of the Health Insurance Portability and Accountability (HIPAA) Rules and other federal laws relevant to health information exchange. In many cases, the resulting variation poses substantial, yet unnecessary challenges to electronic health information exchange. State teams also raised the issue that some entities involved in electronic health exchange are not *covered* under the HIPAA Rules and are not clearly regulated at the state level.

To resolve these issues, some of the state teams are working to achieve consensus on common interpretations of the HIPAA Rules and their applicability within the state. Again, there is a risk that differing interpretations of the same laws will create new barriers to interstate activities. This concern generally extends to federal rather than state laws and regulations, and, clearly, any substantial variation in the state teams' interpretations of the federal regulations would present a material challenge to electronic health information exchange. Although professional organizations and states can assist in interpreting the Privacy Rule and other federal laws consistently, only HHS can issue the kind of authoritative guidance that carries significant legal weight and offers *covered entities* significant legal protection.

This process could be facilitated by HHS's working with the states to produce and publicize appropriate, coordinated guidance on the topics raised by the state teams in this report. HHS agencies and offices can work with the state teams to identify the major areas of ambiguity in the federal law and the underlying causes of ambiguity; prioritize issues on which on guidance is most needed; and produce, publish, and publicize meaningful, authoritative guidance responsive to the examples brought forward by the states (Centers for Medicare & Medicaid, 2007).[21]

In addition, HHS could assist the states in this effort by implementing a feedback mechanism that would allow state organizations to receive specific responses from appropriate federal agencies to questions about potentially ambiguous situations under the federal laws. It is understood that these federal agencies do not have the staff to respond to

[21] CMS's security guidance with respect to the remote use and access to health information is a good example of the type of specific, authoritative guidance that covered entities may rely on.

every specific question that might arise in the health care industry, but, by using the state organizations developed under HISPC to gather and integrate the questions that arise in their respective states, they would have to interact with only about 50 organizations to deal with the most critical and widespread ambiguities that they have prioritized. These same organizations can also multiply the outreach efforts of the federal agencies by disseminating the guidance and answers to specific questions to quickly assuage any rising confusion over privacy and security issues as electronic health information exchanges are implemented in these states and territories.

HHS has taken some good steps in this direction already, although, according to the work of the state teams, additional helpful steps could be taken. As accessed on June 1, 2007, the Office of Civil Rights (OCR) HIPAA Privacy Rule Compliance and Enforcement website includes the statistics of complaints as of April 30, 2007 (OCR, 2007, January 14). The site reports total received complaints (27,070) broken down by the complaints that remain open (22%) and those that have been resolved (78%). In addition, there were 393 referrals to the Department of Justice and 153 referrals to the Centers for Medicare & Medicaid Services. The site does not indicate the status of the referred complaints.

The site also breaks down the resolved cases into those resolved without investigation and those resolved after an investigation. The majority of the cases, 14,297, were resolved without investigation because the complaint *did not present an eligible case for enforcement of the Privacy Rule*. Complaints that fall into this category include complaints where OCR lacks jurisdiction under HIPAA, such as a complaint that alleges a violation prior to the compliance date or a complaint that alleges a violation by an entity not covered by the Privacy Rule. Complaints that are untimely, withdrawn, or not pursued by the filer of the complaint also are considered not eligible for enforcement, as are complaints in which the activity described does not violate the Rule—as when the *covered entity* has disclosed *protected health information* in circumstances in which the Rule permits such a disclosure.

Recommendations are as follows:

- **Recommendation 6.** The appropriate agencies within HHS should work with states to produce and publicize coordinated guidance on topics raised in this report.
- **Recommendation 7.** HHS should implement a program that would allow a single state organization to receive specific feedback and guidance from appropriate HHS agencies.
- **Recommendation 8.** HHS should continue to provide case examples describing common problems and solutions encountered in enforcement cases, as well as richer statistics when they are available.

7.4 Organizational Practice, Policy, and Guidance

The struggle that organizations go through to develop their policies and attendant business practices is very real. It is no surprise that organizations set the bar high to avoid being found out of compliance with something. Although many organizations cited fear of sanctions as motivation for establishing conservative policies, many other organizations cited the business reality that publicized breaches and wrongful disclosures hurt the brand that so many organizations have invested heavily in developing. The complexity of navigating the plethora of policies, statutes, and common law; regulations and mandatory standards; industry standards and guidance to set organizational policy is so great that it is not surprising that organizations arrive at different conclusions or adopt conservative policies to ensure that they are compliant.

Recommendations are as follows:

- **Recommendation 9.** To coordinate the effort to navigate the complexity, HHS should convene a nationwide, public-private effort to define a set of documents to serve as a baseline of common, principle-based privacy and security policies, procedures, and standards to serve as a resource for all entities wishing to participate in an HIE.
- **Recommendation 10.** HHS should convene a nationwide, public-private effort to define a model set of agreements that will serve as the basis for model contracts that all entities participating in HIEs can sign and use to build trust among the participating entities.

With the appropriate support and recognition from the federal and state governments and associated organizations, these model policies, procedures, standards, and contracts could simplify and standardize their implementation across the nation and resolve much of the variation that currently exists. These documents should specifically cover in detail the issues raised as priorities by the state teams.

There are many efforts currently under way that can be leveraged to accomplish these goals. For example, the collaborative work groups being formed as an outgrowth of this project could be coordinated with the Security and Privacy Workgroup of the Health Information Technology Standards Panel (HITSP), the State Alliance for e-Health's Health Information Protection Taskforce, and the AHIC CPS Workgroup. In addition, the Markle Foundation's Connecting for Health project has published documents that can be used as a model under their Common Framework.[22]

The model documents could serve as a starting point for the collaborative work groups who can then work to further develop the model for use as a multistate framework. The inclusion of representatives of states that are not currently part of the HISPC can be of great benefit

[22] The Common Framework (2006) consists of a set of mutually reinforcing technical documents and specifications, testing interfaces, code, privacy and security policies, and model contract language. It was developed by experts in information technology, health privacy law, and policy, and has been tested since mid-2005 by Connecting for Health prototype teams in three states.

to this process. For example, Tennessee has modified and adopted the Connecting for Health documents successfully.

Another model that the collaborative work groups could follow is the work done on the successful Uniform Commercial Code by the NCCUSL. The State Alliance for e-Health could be considered as another potential venue for such work. The goal is not to solve all the problems exactly the same way, but to make it efficient for states to start from an 80% solution, understand their differences from this common baseline, and resolve their unique issues and reduce the variation to a workable level without having to duplicate all the work. This work would also help set technical standards for methods of expressing and implementing patients' desires to control their own health information.

7.5 Technology and Standards

A high priority for the state project teams is identifying, evaluating, and adopting standards for private and secure health information exchange. As indicated elsewhere in this report, knowledge of work being done at the federal level with regard to interoperability standards is lacking at the state level. In the absence of widely adopted electronic standards, states and health care organizations will continue to move in many directions, utilizing different methods, modes, formats and technologies that are, in many cases, incompatible and noninteroperable. Currently there are two main nationally recognized processes for the selection, adoption, and implementation of such electronic standards. The first is the HITSP which is working to harmonize interoperability standards, including those specifically related to electronic health information privacy and security. The electronic standards being harmonized are developed and maintained by national standard-setting bodies, such as ASTM International, OASIS, DICOM, IEEE, IETF, ANSI Xn, FIPS, NIST, HL7, IHE, and others.[23] In addition, international standards (such as the Organisation for Economic Co-operation and the International Organization for Standardization) and privacy and security frameworks are being considered. The second is the Certification Commission for Healthcare Information Technology (CCHIT), the national organization developing certification evaluation criteria and implementing a nationally recognized certification process for electronic health records products and services provided by health information network providers.

It will be important to bring the HISPC collaborative work groups together with HITSP and CCHIT to ensure consistency in the implementation of electronic health information security and privacy standards. One way to accomplish this would be to facilitate outreach and education efforts by both HITSP and CCHIT to the state teams to increase the level of

[23] OASIS = Organization for the Advancement of Structured Information Standards; DICOM = Digital Imaging and Communications in Medicine; IEEE = Institute of Electrical and Electronics Engineers; IETE = Institution of Electronics and Telecommunication Engineers; ANSI = American National Standards Institute; FIPS = Federal Information Processing Standards; NIST = National Institute of Standards and Technology; HL7 = Health Level 7; IHE = Integrating the Healthcare Enterprise.

awareness and understanding of the role, responsibilities and activities of both HITSP and CCHIT, and how they relate to local, regional and state health information exchange initiatives.

7.6 Specially Protected Health Information

The state teams identified a need to develop a standard approach to managing the exchange of *specially protected health information*. While the HIPAA Privacy and Security Rules consider all health information equally sensitive (with the exception of psychotherapy notes), there are a number of other federal and state laws that do single out specific types or classes of health information as needing special protections. The special protections generally require the patient's express permission to use or disclose the *specially protected health information* for any purpose. Organizations, in turn, have developed and implemented a wide variety of procedures, practices, and use of security technologies to achieve their policy goals of confidentiality, integrity, and availability in the handling of specially protected classes of data.

State teams generally advocated for 1 of 2 approaches. One approach was to treat all health information as equally sensitive and apply the same level of protection across all classes of information; the second approach advocated the need to maintain the higher standard of protection for certain classes of information, which would require the development of a clear standard for identifying and classifying specially protected data elements and the conditions under which the information could be exchanged. To do so would require establishing a clear system of classification of health information so that appropriate privacy and security measures could be applied to each class of information, consistent with the requirements and needs defined for that class.

Many sensitive information classification models already exist in the private sector and government. Numerous health care organizations developed information classification schemas, most of which are simple 2- or 3-level identification systems (eg public data, confidential data on organizations, private data on individuals, specially protected data on individuals). But even though these schemas exist, most current electronic health information applications (such as EHRs) do not easily accommodate such data segregation at different levels of granularity. This difficulty of accommodation is especially true regarding chart notes that are not structured so as to allow easy "redaction" of *specially protected health information* when necessary. In addition, these schemas do not, from the patient's perspective, account for what health information might be considered in need of special protections.

To accomplish this approach means that a comprehensive assessment of *specially protected health information* must be undertaken, which would require an inventory of federal and state laws to identify those classes of information that are specially protected and analysis

of the handling requirements. Based on the assessment, a common framework for identifying, defining, classifying, and managing *specially protected health information* could be developed and vetted with stakeholders. Developing the classification is no simple task. Protecting a diagnosis of HIV but not a test result or a prescription that by inference would reveal the diagnosis becomes a monumental task. In addition, decisions must be made about whether patients will have the right to determine what qualifies for protected status in their records. Given the vast range of purposes for which health information can potentially be used and disclosed, the initial assessment should focus on a limited set of standard purposes, such as treatment, payment, health care operations (such as quality review), and research. Finally, this topic should be a priority for coordination among the state teams and the HITSP and CCHIT. Specific emphasis should be made on how the harmonized standards allow entities to electronically meet the requirements of current laws that afford special protections to information such as HIV/AIDS, sexually transmitted diseases, mental health, substance abuse, and genetic information. CCHIT, in particular, should explore how EHR products will include functionality that allow handling of sensitive health information.

7.7 Adoption of Privacy Policies and Security Standards

State teams are also struggling with the question of how to ensure adoption and enforcement of agreed-on privacy policies and security standards by stakeholder organizations. The approach used may largely depend on the specific policies or standards being adopted. For example, the state teams discussed the need for standard approaches for documenting and managing patient *consent*. This measure would require that the state teams first adopt standard interpretations of the various federal and state laws and regulations governing *consent*. There are also technology standards necessary to implement privacy policy (eg, electronic *consent* management, access controls) and security standards (eg, user/entity authentication, authorization, access controls, audit, nonrepudiation) that conform to federal and state laws and regulations and are reflective of business practices, policies, and procedures.

In the United States, the methods for adopting and using standards in any given industry have generally followed 1 (or more) of the following paths, depending on the type of industry, type of transaction, market conditions, and level of maturity of standards:

- “de-facto” standards that market forces identify and industry organizations adopt and begin using (“de-facto” adoption);
- national standards that an accredited national standard-setting body has identified and that the industry embraces and uses (consensus adoption);
- establishment of industry-driven credentialing requirements for products and services to adopt and use specific standards (credentialing adoption);
- use of purchaser power or public program authority to create incentives or even require the use of specific standards (purchaser-based adoption); and

- establishment of state or federal regulations that identify specific standards the industry is required to adopt and use (regulatory adoption).

A variation of the purchaser-based adoption is the recently issued Executive Order (14310), that directs federal agencies to (1) ensure that as each agency implements new or upgraded health information technology systems, those systems utilize products that meet recognized interoperability standards; and (2) ensure that each agency requires in contracts or agreements with health care providers, plans, or insurers, that, as each provider, plan, or insurer implements new or upgraded health information technology systems, those systems also utilize products that meet recognized interoperability standards.

Similar approaches may be needed to assist states in achieving widespread adoption of standard approaches to privacy and security. Close coordination between the states and the HITSP and CCHIT will be helpful in expanding the adoption of the harmonized privacy and security standards. Similarly, state teams can work with other health care accrediting bodies (ie, Joint Commission on Accreditation of Healthcare Organizations, National Committee for Quality Assurance) to ensure that privacy and security standards are adopted and incorporated, as appropriate, into their respective accrediting requirements and processes. Finally, state teams could work with other national purchasing coalitions and groups to create a “Pay for Conformance” campaign and strategy aimed at ensuring that health care organizations (providers, health plans, and others) adopt and use recognized privacy and security interoperable standards.

7.8 National Privacy and Security Health Information Resource Center

The ever growing wealth of data and information available to the health care industry on health information privacy and security is staggering. Navigating through this sea of information can be overwhelming, confusing, or even intimidating. Finding the right information in a reliable and timely manner can be a difficult task. A simple search on the term *Health Information Privacy* in the Knowledge Library of AHRQ’s National Resource Center for Health Information Technology provides over 36,000 entries.

The fast pace of developments in this field has created the need to develop a privacy and security national resource center, in order to consolidate, organize, normalize, and present this comprehensive body of information in a manner that is easily accessible, efficiently searchable, and effectively used by the industry. The center would serve as a way to increase collaboration and education among national, regional, and state work groups and organizations. Information could be organized by the target audiences, which would include consumers, health care providers, health plans, researchers, public health, policy makers, governmental units (ie, law enforcement, courts, correctional institutions, military), healthcare clearinghouses, and vendors, among others.

The recommendation is as follows:

- **Recommendation 11.** Create an Internet-based national resource center for health information privacy and security. The primary purpose of the national resource center would be to provide reliable, unbiased and timely information about health information privacy and security to the health care industry.

7.9 Consumer Outreach, Engagement, and Education

The need for outreach, engagement, and education of stakeholders about electronic health information exchange and issues of privacy and security emerged as a key issue over the course of this project. Solutions offered ranged from local approaches and state approaches to national-level initiatives. Initiatives to engage and educate health care stakeholders about the significance of private and secure interoperable health information exchange must have several important characteristics. First the initiatives must be continual. Education and outreach are not a 1-time effort. They should be made available on an ongoing basis, particularly given the evolving health information technology environment. Second, initiatives must be accessible. Education and outreach initiatives must be easily accessible to the intended audience. Third, the initiatives must also be scalable. Many factors affect the content and delivery of education and outreach efforts, including target audience characteristics; familiarity with the health care system; and federal, state, and local regulatory considerations. The content and scope of education and outreach activities must be comprehensive enough to fulfill the needs of the intended audiences. Finally, addressing health information privacy and security in the context of new and evolving HIT applications, such as EHRs, personal health records, and health information exchanges will require the deployment of a comprehensive industry outreach and education campaign at the national level.

Consumers are one of the core stakeholder groups most affected by electronic health information exchange, and, therefore, consumer engagement is a critical component of this work. If meaningfully engaged in the planning and development of electronic health information exchange initiatives, consumers will be vested in the process and can be the driving force necessary to move this effort forward. As noted at the national meeting, consumers and consumer groups can be effective lobbyists for the legislative support of health information exchange initiatives, including obtaining funding.

On the other hand, if health care consumers are not engaged in this issue, they will not trust that their information will be protected and under their control, and they will not fully embrace the system and the opportunity to leverage consumer input will be lost. As they worked to engage consumers in the process, state teams learned an important lesson: health care consumers, in general, were not aware of health information exchange initiatives and the implications; therefore, they did not necessarily feel that they could productively participate in the work. Although special classes of health care consumers,

such as patients with chronic or debilitating disease, were more knowledgeable about health information exchange and EHRs, the state teams still had difficulty engaging them in the process.

Many state teams proposed focus groups to vet some of the work with small groups of consumers. Although such groups may have met the needs of the current project, reliance on focus groups will not serve the long-term goal of engaging health care consumers as fully participating stakeholders who are actively engaged in developing privacy and security requirements for health information exchange. Early in this process we recognized this issue and asked representatives from the National Partnership for Women and Families (a nonprofit, nonpartisan advocacy group dedicated to promoting fairness in the workplace and access to quality health care) and the National Consumers League to attend the regional meetings and discuss ways that the state teams could bolster their efforts to engage consumers. Both organizations are part of a growing coalition dedicated to encouraging consumer education and involvement in developing health information exchange initiatives. Both organizations recommended that the state teams engage state advocacy organizations to leverage the existing constituencies and outreach mechanisms; they also noted that these organizations will have to be educated and funded.

The proposals and experiences of the states, as well as the recommendations of these national consumer organizations, highlight needs in three main areas that could potentially be addressed at the national level.

7.9.1 Developing Processes for Involving Consumers and Consumer Groups in the Planning and Development of HIEs

HIE initiatives would benefit from the development of effective community consultation processes to ensure that health care consumers will be involved in the planning process at an early stage and remain engaged throughout HIE development. This means both informing consumers about existing health information exchange practices, as well as the privacy and security implications of moving to widespread electronic health information exchange. Although community consultation is probably best known in the United States as a way of obtaining community input on research involving emergency care where obtaining informed consent is impossible, examples exist of using this process to make policy decisions in other arenas, including the development of HIE systems. For example, each of the three communities involved in a pilot project of the Massachusetts e-Health Collaborative (MAeHC; 2005) utilized consumer councils to obtain patient/consumer input in the development of their local HIE (2007). Considering the experiences of MAeHC and other HIE projects, HHS could work to develop and make publicly available a suggested framework for states and regions to use to conduct community consultation on the development of an HIE, which includes education on existing HIE practices. A good example of such guidance (although addressing another issue) is the report, Ideas for Community

Consultation, issued by New South Wales Department of Urban Affairs and Planning to facilitate the urban planning process in that Australian state (2001).

The federal government could also adopt a more formal community consultation approach to ensure that the concerns and needs of consumers are met and that unrealistic expectations are not set. Two potential models for this kind of national consumer consultation have been used in England, where an annual public meeting is held to educate and obtain feedback from citizens on their developing nationwide HIE (NHS Connecting for Health, 2007),[24] and Australia, where the Consumer's Health Forum, a national organization that can reach nearly 1 million Australians, has worked with the government to ensure a high level of consumer input and engagement for the development and implementation of EHR systems in that country (Consumers' Health Forum of Australia, 2003).[25] A workable model here might take advantage of the web panels composed of health care consumers, like those used for online surveys and polls.

Recommendations are as follows:

- **Recommendation 12.** A publicly available framework should be developed for states and regions to use to conduct community consultation on the development of HIE.
- **Recommendation 13.** The federal government should also adopt a more formal community consultation approach to ensure that the concerns and needs of consumers are met.

7.9.2 Educational Materials Targeted to Consumers

Health care consumers and consumer groups, some of the most affected stakeholders in the development of electronic health information exchange, cannot be meaningfully engaged in this process if they are not adequately informed. While some efforts have been made to educate consumers and consumer groups on issues surrounding HIT and health information exchange, they are few and barely begin to address the need.

Before a comprehensive education package is developed, it is critical to learn what consumers know and do not know about how their records are currently stored and what the privacy and security implications are for moving to EHRs and electronic health information exchange. There have been a number of brief web surveys conducted that are of little value for a number of reasons, including poorly constructed questions. Because the reports do not describe the sample selection methods or response rates, there is no way to tell if the results can be generalized beyond those surveyed. To understand what consumers think about these very important issues will require collecting information by using rigorous questionnaire development and testing methods and a sample of health care consumers

[24] Presentations of the latest national conference can be found at the website (NHS Connecting for Health, 2007).

[25] Information on the e-Health for Consumers project is available at the website (Consumers' Health Forum of Australia, 2003).

selected through a probability-based sampling methodology. In addition, the sample should be of sufficient size to perform some subgroup analyses based on demographic variables, such as racial and ethnic minority status, urbanicity, and geography: consumer trust in the health care system is known to vary across these dimensions. Only then will we be able to make decisions about how best to address the issues of concern to the American public.

In general terms, educational materials for consumers and consumer groups must explain in neutral, lay terms concepts and models (eg, HIEs, personal health records, EHRs, federated systems, centralized systems); benefits and risks associated with different HIE models; various privacy and security measures (eg, role-based access). The materials must also elicit the questions that consumers want to ask during the process of developing local HIE. The development of these materials should be undertaken with extensive consultation with consumers and consumer groups to ensure that the materials appropriately meet their needs and that these groups are fully vested in promoting the use of these materials. The privacy and security resource center proposed earlier could be a venue to make these materials widely available.

7.9.3 Facilitating Involvement of Consumer Organizations

Consumer organizations can be powerful advocates for ensuring that health care consumers receive clear, unbiased information about the issues of most concern to them. Most consumer groups operate largely with grant funding, which is often restricted to a specific project. Grants are often obtained from foundations that have specific areas of interest. With few exceptions, electronic health information exchange does not fit squarely within the project areas funded by most foundations. Even foundations that fund health-related projects often focus on what are perceived as the most currently pressing issues of the day, such as ensuring access to care. Health information exchange is generally perceived as a less pressing issue for which the payoff is comparatively remote.

However, since electronic health information exchange will be a key driver behind improving quality of care and reducing health care costs, it is important that this topic become a priority for these organizations. One way to ensure this outcome is to develop and make publicly available materials that support the business case for consumer organizations seeking new funding or allocating already scarce resources to electronic health information exchange issues, particularly those with respect to consumer education.

REFERENCES

Brewin B, Ferris N. Master index pitched as patient ID alternative. *Government Health IT*. Sept 12, 2005. http://govhealthit.com. Accessed May 12, 2007.

Bureau of National Affairs. Does HIPAA preemption pose a legal barrier to health information transparency and interoperability? *BNA Health Care Policy Report* 15. 2007:11.

Centers for Medicare & Medicaid Services. Security standard overview. 2007. Available at: http://www.cms.hhs.gov/SecurityStandard/. Accessed May 12, 2007.

Conn J. Paper records more secure. *Modern Healthcare Online*. May 2, 2007. http://www.modernhealthcare.com. Accessed May 10, 2007.

Consumers' Health Forum of Australia. 2003. E-Health for Consumers Project 2006-08. Available at: http://www.chf.org.au/projects/. Accessed May 10, 2007.

Creswell JW. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (2nd Edition).* Thousand Oaks, CA: Sage Publications; 2003.

EHealth Initiative and Foundation. 2007. EHealth Initiative's Connecting Communities Toolkit. Available at: http://toolkit.ehealthinitiative.org/communication_and_outreach/tools_marketing.mspx. Accessed May 10, 2007.

Foundation of Research and Education (FORE). January 12, 2007. Development of consensus best practices for state-level regional health information organizations [report transmittal letter and recommendations to Secretary Leavitt].

Kemmis S, Wilkins M. Participatory action research and the study of practice. In: Atweh B, Kemmis S, Weeks P, eds. *Action Research in Practice: Partnerships for Social Justice in Education*. London: Routledge; 1998:21–36.

Markle Foundation. 2006. Connecting for Health Common Framework webpage. Available at: http://www.connectingforhealth.org/commonframework/index.html. Accessed May 12, 2007.

Massachusetts eHealth Collaborative (MAeHC) website. 2005. Available at: http://www.maehc.org/. Accessed May 12, 2007.

New South Wales Dept of Urban Affairs and Planning. *Ideas for Community Consultation*. 2001. Available at: http://www.planning.nsw.gov.au/planfirst/pdf/principles_procedures_final.pdf. Accessed May 10, 2007.

NHS Connecting for Health. Care Record Development Board webpage. 2007. Available at: http://www.connectingforhealth.nhs.uk/crdb. Accessed May 10, 2007.

Office for Civil Rights website (OCR). January 29, 2007. Available at: http://www.hhs.gov/ocr/hipaa. Accessed May 10, 2007.

Office for Civil Rights (OCR). HIPAA Compliance and Enforcement webpage. January 14, 2007. Available at: http://www.hhs.gov/ocr/privacy/enforcement/. Accessed May 10, 2007.

Strauss A, Corbin JM. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques.* Thousand Oaks, CA: Sage Publications; 1990.

Strauss A, Corbin JM. *Basics of Qualitative Research (2nd Edition): Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: Sage Publications; 1998.