December 29, 2006

Privacy and Security Solutions for Interoperable Health Information Exchange

Interim Assessment of Variation

Prepared for

Susan Christensen, Senior Advisor
Agency for Healthcare Research and Quality
540 Gaither Road
Rockville, MD 20850

Jodi Daniel, Director, Office of Policy and Research
Office of the National Coordinator
330 C Street SW
Switzer Building, Room 4090
Washington, DC 20201

Prepared by

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

Contract No. 290-05-0015
RTI Project Number 0209825.000.004.002

RTI Project Number
0209825

Privacy and Security Solutions for Interoperable Health Information Exchange

Interim Assessment of Variation

December 29, 2006

Prepared for

Susan Christensen, Senior Advisor
Agency for Healthcare Research and Quality
540 Gaither Road
Rockville, MD 20850

Jodi Daniel, Director, 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

List of Authors for Summary Report

Amoke Alakoye, MHS, RTI International
Chris Apgar, CSSP, CISSP, Apgar & Associates
Robert F. Bailey, BA, RTI International
William Braithwaite, MD, PhD, Braithwaite Healthcare Consulting
John Christiansen, Christiansen IT Law
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
Stephanie Rizk, MS, RTI International
Walter Suarez, MD, CEO, Institute for HIT/HIPAA Education and Research

List of Reviewers

Holt Anderson, Executive Director, NCHICA
Ryan Bosch, MD, George Washington University Medical Faculty Associates
Gary Christoph, PhD, CIO, Teradata
Carolyn Hartley, Physicians EHR
John McKenney, SEC Associates
Kathleen Nolan, Director of Health Policy, Center for Best Practices, National Governors Association
Anna Orlova, Public Health Data Standards Consortium
Joy Pritts, PhD, Health Policy Institute, George Washington University
Harry Rhodes, MBA, RHIA, CHPS, AHIMA
Michelle Lim Warner, MPH, Center for Best Practices, National Governors Association

Contents

Appendices

Tables

EXECUTIVE SUMMARY

This report is the first in a series to be produced under RTI International's contract with the Agency for Healthcare Research and Quality (AHRQ). The contract, entitled Privacy and Security Solutions for Interoperable Health Information Exchange, is managed by AHRQ and the Office of the National Coordinator for Health Information Technology (ONC). The following report is a summary of 34 separate interim reports submitted by 33 states and one territory as subcontractors to RTI; these subcontractors form the Health Information Security and Privacy Collaboration (HISPC). The Interim Assessment of Variation of Business Practices, Policies, and State Law (IAV) comprises the first reports submitted by the 34 subcontracted state teams and represents a "first look" at the major areas states have identified as presenting challenges to the privacy and security of electronic health information exchange (eHIE). This summary report captures the highlights from the 34 reports and presents some of the major crosscutting themes that have been raised during this first phase of the project.

This summary report consists of 3 major sections:

- Methodology
- Descriptions of Business Practices by Scenarios
- Critical Issues and Observations

The purpose of the IAV is to illustrate, in a descriptive report, the variations among the organization-level business practices, policies, and laws, as related to privacy and security, that were identified by each state team. The term *law* as used here refers to regulatory, statutory, or case law that serves as the primary driver behind a business practice. The data supporting this report come from work conducted by the Variations Work Groups (VWG) and Legal Work Groups (LWG) of each participating state team. The interim reports will be used to inform efforts of the Solutions Work Groups (SWG) and Implementation Planning Work Groups (IPWG) as the state teams continue to draft their interim reports. It is important to note that the interim reports are but a "snapshot" of a point in time in an evolving process as the state teams work with stakeholders to think through the multitude of privacy and security issues related to eHIE and as they work toward developing privacy policy and security standards to address the needs of their local communities.

Although each state team followed a core methodology, ample opportunity remained to tailor the process to meet the needs of each participating state and territory. The reports include a section that documents the process used to generate the set of organization-level business practices for each scenario, including outreach to the broader stakeholder groups, and a description of the membership and stakeholder representation of the VWGs and LWGs.

The descriptions of business practices in each of the HISPC reports are organized by 11 purposes for health information exchange (HIE), as shown in Table ES-1. These purposes represent clusters of the 18 scenarios used to drive the discussions of business practices. Within each of the 11 sections, each state team was asked to provide a description of (1) the stakeholders who provided input to the collection of business practices; (2) the major domains addressed by the business practices (based on the 9 domains of privacy and security) including a discussion of the relevant policy, legal drivers, or rationale behind the practices; and (3) critical observations not offered elsewhere in the report.

Table ES-1. Purposes of Health Information Exchange (HIE) and Relevant Scenarios

Purposes of HIE	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

Finally, each state report provided a summary of the critical observations and key issues to bring focus to areas that the SWGs and the IPWGs should further explore.

In Section 3 we describe 10 issues that have been raised by the state teams in the interim reports and that have broad implications for nationwide eHIE. This section provides a brief overview of these topics, which is not intended to be a thorough analysis of the issues or their implications but rather a descriptive treatment of the issues. The expectation is that additional issues will be raised as the work continues and a fuller explication of the implications will be provided in the final Assessment of Variation and Analysis of Solutions reports.

HIPAA Privacy Rule Interpretations and Applications

Many business practice variations existed because of different interpretations of the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Privacy

Rule. The most commonly mentioned was variability in the use and implementation of patient consent or authorization across organizations. Many of the reports indicate a lack of understanding on the part of the stakeholder community about the HIPAA philosophy that the privacy rules are not intended to create any barrier to the use of personal health information for treatment of the patient and that patients should expect their information to be routinely used for purposes of treatment, payment, and health care operations (TPO) unless exceptions are negotiated with the provider. Others seem to understand this approach but see conflicts with traditional practices and local laws, or at least variability in the processes of implementing practices. Section 3.1 summarizes key examples from the states regarding specific HIPAA-infused barriers to eHIE.

HIPAA Security Rule Interpretations and Applications

A review of state reports indicated some confusion and misunderstanding surrounding what appropriate security practices are, but also indicated misunderstandings regarding what was currently technically available and scalable to the health care industry and consumers. This lack of knowledge, understanding, and trust between organizations and on the part of consumers was more evident in the business practices than in state laws. For the most part, state laws did not pose challenges to sound security, nor did the HIPAA Security Rule. Sometimes the matter was simply that, even though HIPAA accommodates scalability in security programs, organizations voiced concern related to liability when one organization that believes its security program is more robust sends protected health information (PHI) to another organization with a less robust security program.

There also appeared to be confusion about the different types of security required by the HIPAA Security Rule. The Security Rule addresses administrative, physical, and technical security. Even though more than one third of the rule addresses administrative security requirements, many organizations focused more attention on needed technology than on administrative safeguards.

Trust in Security

Trust was a critical issue raised in many of the state reports, as it affects the potential viability of eHIE. Specifically, 2 kinds of stakeholders expressed concerns: providers and consumers. Providers were principally concerned about liabilities possibly arising from the activities of other participants in HIE and about consumers' lawsuits for inappropriate disclosures of their information; they were concerned secondarily about potential uses of information about consumers by payers and the government. In contrast, consumer concerns tended to focus on privacy risks arising from the implementation of new technologies and the potential for unauthorized disclosures of sensitive information to payers and employers.

The leading trust issue was providers' fear of lawsuits and liabilities associated with eHIE. 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 HIE. One state team identified this fear as its single most significant issue, one which had been repeatedly raised and the reason providers were not willing to engage in eHIE. It is not clear whether there is much experiential basis for this fear in most states, but one identified as a concern a specific statute giving patients a cause of action for inappropriate disclosure, and another reported that HIPAA-based claims are being included in lawsuits by patients frequently enough that one provider had reported 6 such claims within the preceding 6 months. (The specific legal basis for such claims was not identified. HIPAA does not provide a cause of action for individuals.)

The second most significant trust issue was consumer lack of trust, which appeared to have been expressed directly by consumers in 4 reports and was apparently 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. It appears that one major reason for this sense of mistrust is the substantial number of security breaches that have been reported over the last few years, including several involving health care organizations.

The most significant general impression that arose from this review was that trust concerns, particularly of providers, appear to be directly correlated with eHIE experience. In other words, providers in states with relatively few eHIE activities, or a briefer history of such activities, appear to fear they may be held liable or be penalized for engaging in them and, in some cases, do not trust the technologies. Providers in states with more experience in eHIE do not report the same concerns, or they report them to a lesser degree.

Finally, one noteworthy finding is that 2 state teams reported reliance on good faith and personal relationships in current practices and identified this as a positive value participants wish to preserve.

State Laws

The stakeholders identified a number of difficulties with the state laws governing privacy and security, including a general misunderstanding of the intersection between state law and HIPAA, as well as some general confusion about where state law was found and how it should be applied. In addition, when state law was readily identified and understood, it was often too antiquated to apply sensibly to eHIE.

In fact, the leading issue was the absence of state laws clearly applicable to eHIE (sometimes referred to in the reports as "laws pertaining to RHIOs" [regional health information organizations]), which was identified by 11 state teams. Ten state teams identified the generally confusing conditions of state laws as a critical issue, and,

consistently, 11 state teams reported the use of overly conservative business practices due in large part to confusion or lack of knowledge about state laws. ("Overly conservative" in this context means more restrictive in terms of information sharing than is actually required by law.)

At least 2 states noted that a number of stakeholders, particularly providers, were unaware of the need to comply with state laws that are more restrictive than HIPAA and were, in effect, treating HIPAA as a ceiling rather than a floor. One caveat in reviewing these reports for awareness of state law is that state teams were asked to identify only state laws that provided the underlying rationale for a specific business practice; they did not engage in a comprehensive legal analysis of their entire body of state law governing privacy and security. Confusion about sharing information for law enforcement, public health, and bioterrorism purposes, in particular, appears to be a critical problem, given concerns about possible bioterrorist incidents, natural disasters, pandemic flu, and other mass crises. Current practices appear to rely heavily on good will, which is necessary but perhaps not sufficient, especially when interstate coordination is necessary.

Intersection With Other Federal Laws and Regulations

The state reports included a number of examples of challenges involving the intersection of state laws with HIPAA and other federal laws and regulations.

In the early 1970s, Congress recognized that the stigma associated with substance abuse and fear of prosecution deterred people from entering treatment, so it enacted legislation that gave patients a right to confidentiality. For the almost 3 decades since the federal confidentiality regulations (42 C.F.R. pt. 2) were issued, confidentiality has been a cornerstone practice for substance abuse treatment programs across the country. These regulations protect all information about any person who has applied for or been given diagnosis or treatment for alcohol or drug abuse at a federally assisted program. The 42 C.F.R. pt. 2 regulations generally require patient consent (authorization) prior to disclosure of information, except in emergency situations.[1] These restrictive requirements pose a challenge to the exchange of health information.

There are differences in providers' treatment of patient medical information when substance use is involved: variation exists in the treatment facilities', physicians', and integrated delivery systems' understanding of 42 C.F.R. pt. 2, understanding of the relation of 42 C.F.R. pt. 2 to HIPAA, and the application of each. Treatment facilities note stringent precautionary measures to safeguard patient substance use information: while physicians comment on limited or restricted access to patient medical files, treatment facilities note that patient files are kept in a locked cabinet behind a double-locked door.

[1] *Consent* is the term used in 42 C.F.R. § 2.31, "Form of written consent."

The state reports show that, although the stakeholders representing treatment facilities in participating states demonstrate a general understanding of 42 C.F.R. pt. 2, other health care providers are less familiar with the regulation's requirements. The complicating factor is that the differences between HIPAA provisions and 42 C.F.R. pt. 2 provisions create ambiguity about which regulation applies and under what conditions. Consequently, variation in both policy and practice increases across an array of stakeholders. The differences in language and drivers for each regulation create further ambiguity, leading to increased variation in how the regulations are applied by stakeholder organizations. The result in current practice is that, without a provider's clear understanding of the requirements for both HIPAA and 42 C.F.R. pt. 2, protected information might be shared because that provider understands that HIPAA allows sharing of health information for treatment, even though sharing without patient authorization would be prohibited under 42 C.F.R. pt. 2.

One state team referred to Clinical Laboratory Improvement Amendments (CLIA) as a barrier to eHIE. CLIA defers to state law for the purpose of determining the permissible recipients of laboratory results. Many state laws very narrowly define those persons who are authorized to receive test results, and variation among state laws has created a medley of different standards.

Under CLIA regulations, 42 C.F.R. § 1291(f) states, "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 there is significant uncertainty as to its meaning.

One state team also raised as a potential barrier to electronic prescription data exchange the federal regulation 21 C.F.R. § 1306.11, which requires that the original, written, signed prescription be presented to the pharmacist for review before the dispensing of a controlled substance. Another state team mentioned the Employee Retirement Income Security Act of 1974 and wrote that "the limit and boundaries of the Employee Retirement Income Security Act, 1974 are not clear" in relation to state law; there was also a mention of the Family Educational Rights and Privacy Act.

Networking Issues

Most state teams reported quite limited interorganizational exchanges of clinical information being done electronically for 3 reasons: (1) absence of regional eHIE networks, (2) limited deployment of electronic health record (EHR) systems, and (3) lack of interoperability in those EHR systems that have been deployed. eHIE between organizations is limited mainly to content-specific clinical messaging in the areas of pharmacy/prescription drug information (e-prescribing), laboratory data, and radiology/digital imaging data. Across

many states a significant number of pilot projects are under way to test various eHIEs, including emergency department data and public health data.

Significant capacity gaps and variations exist in the level of resources, technical capabilities, and financial means of organizations (ie, large versus small, urban versus rural). These gaps create significant variation in HIE practices among organizations; in turn, these variations in HIE practices limit or restrict the ability of organizations to conduct interorganizational HIEs (lack of compatible systems, lack of compatible practices, lack of trust). State teams also noted that different types of HIE (ie, provider-to-provider, provider-to-payer, payer-to-payer, and between others) require different handling.

Individual states are at very different stages in the development of networks that facilitate the interorganizational exchange of clinical health information electronically. Some states altogether lack initiatives to establish such network infrastructures; some are beginning to organize their communities, but no infrastructure approach has been identified, selected, or adopted; some have implemented limited-scope efforts to connect a small number of organizations within a region in the state (subregional networks); and only a very few have a state network infrastructure. A common concern across state teams was the lack of well-defined, operational, and deployable models for regional networking.

There are many definitions of what RHIOs are and many definitions of their roles, functions, funding structure, and so on. There were significant concerns among the state teams about the legal status of such organizations, their ability to legally operate such eHIEs, their ability to store and maintain data, and the like. This lack of experience with organizations designed to govern electronic data exchange, as well as the uncertainty about their legal status, carries implications for stakeholders seeking to design and put into practice consensus-based privacy and security solutions: such organizations could serve as the mechanism by which many decisions are implemented and enforced.

Linking Data From Multiple Sources to an Individual

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

Patient and provider identification across organizations is required in order 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 HIEs 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 eHIE functionality.

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

The variability in methods across organizations to match patients to their records and the lack of agreed-upon patient-to-record matching standards to apply during interorganizational HIEs were perceived as major challenges by many state teams. This was not the case for 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, or NPI).

Current practices reported by participating stakeholders from most state teams pointed at organizations' use of unique, asynchronous, and incompatible methods to establish the identity of their patients, enrollees, clients, and consumers. State teams reported instances in which even within an organization the same patient had been assigned more than one ID within that organization (eg, a patient's ambulatory or primary care clinic record vis-à-vis the same patient's inpatient or hospital record). Although multiple IDs for the same patient are 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. Most state teams also emphasized the need to establish standard mechanisms to identify patients across organizations as a foundational component of the evolving eHIEs.

State teams specified challenges associated with the variability and incompatibility of patient identification systems and approaches, including

- 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 health care systems (public health functions); and
- 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 information available on him or her instead of using automated methods to aggregate the information across sources.

The state teams were acutely aware of the potential risk increase for privacy violations and identity theft when a unique patient ID is implemented across institutions or regions. State teams also cited the need to counter possible negative public reaction with effective security controls and extensive consumer education.

Interstate Issues

Although the identification of interstate issues was not a primary focus of the interim assessment of variation, 16 state teams reported that interstate issues should be considered carefully, though it is not clear that the issues cited posed critical barriers to eHIE. Typically, states raised interstate issues for one of two reasons: (1) either there is considerable sharing of health care facilities across state lines, or (2) whenever the state experiences very large seasonal inflows of both out-of-state workers and tourists its residents make substantial use of out-of-state providers and a number of interstate health systems and plans have facilities and do business in the state.

One markedly rural state noted that, because of its relative scarcity of certain kinds of health care facilities, access to other states' hospitals and specialty services is crucial for its residents; in fact, for this state any meaningful health information infrastructure would have to reach major metropolitan areas in 3 other states. The legal variations noted as potential barriers to eHIE include differences in standards for genetic information; electronic prescriptions; immunization, HIV/AIDS, and minors' rights; minors' consents; and workers' compensation, mental health, and substance abuse.

In addition to reporting interstate issues, at least one state team reported that agreement to reduce variations between state and American Indian tribal standards is critical to developing statewide eHIEs. Several state teams noted that they did not believe that interstate issues were problematic and indicated that the disclosing state's law generally controlled. Most issues were between organizations rather than between states, and interstate issues tended to be resolved within organizations.

Disclosure of PHI

Overall, state teams consistently identified the business practice variations related to the disclosure of health information as the single most significant set of factors affecting the ability to conduct eHIE between organizations. Disclosure-related factors affecting eHIE, as identified by states in their interim reports, are

- general lack of consistent and accurate understanding of federal and state laws and regulations with respect to disclosures, as well as the corresponding effect on the variability of business practices;
- issues surrounding the interpretation, requirement, and use of patient consent or patient authorization in connection with the release of health information;
- issues related to the re-release or redisclosure of health information received by one entity from another;
- issues related to the HIPAA *minimum necessary* requirement;
- issues of ownership and control of health information;
- differences in the way certain health information must be treated and handled because of local, state, and federal regulations that consider that kind of information to have a higher degree of sensitivity;
- the need to ensure that under medical or health emergency circumstances health information is able to be exchanged fast, easily, and securely;
- varying degrees of reporting requirements for public health purposes;
- handling of disclosures related to judicial proceedings and law enforcement;
- burden imposed by the need to document certain disclosures of health information; and
- other issues, including importance of human judgment factor in determining disclosure, and the validity, applicability and acceptability (legal and otherwise) of digital signatures to support patient consent and patient authorization procedures.

Cultural and Business Issues

State teams referenced a number of cultural and business issues that pose challenges to eHIE. 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. At least one state's patient consent requirements place all responsibility and liability for the appropriate release of patients' health information on the health care provider *releasing* information and place no responsibility on health care providers *requesting* the information.

Another example of a business issue that poses a challenge is general resistance to change, which is a common issue that organizations face whenever there is a change in how business is conducted. This is frequently cited as a cultural issue in discussions about decisions to adopt electronic systems. There is a certain comfort with existing paper-based or manual systems and data exchange practices and processes, and there is a general belief that current manual practices are timely, effective, and productive of accurate data. Implicit in some of the discussions is an assumption that security slows down the process, in the sense that the data are secure but are not transmitted as fast as they can be with a quick phone call.

In fact, most exchanges occur person to person, especially in emergency situations, and human judgment plays a large role in how and when information is exchanged. It will be crucial to include these points at which human judgment is required in the specifications for any system developed to exchange information.

Technology adoption gaps (large versus small, urban versus rural), costs of systems, processes to address security domains, and lack of resources must also be addressed.

A third 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 serve to increase variation as organizations attempt to meet compliance by defining terms in ways that protect the interests of the organization. For example, there is the term *health record*. Disagreement exists 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*.

Another cultural issue that was raised involves the tension between health care providers, hospitals, and patients concerning who controls or owns the data. A number of providers indicated that they did not think that patients should have full access to their records, especially to doctors' notes. A concern was that doctors would not enter complete notes if the patient would be able to access the record. Concerns about liability also emerged. Despite these concerns, the majority of stakeholders agreed that eHIE should be designed in ways to address patients' needs, interests, and concerns and that doing so is critical to the success of eHIEs.

1. METHODOLOGY

In June 2005 the U.S. Department of Health and Human Services published the *Summary of Nationwide Health Information Network Request for Information Responses,* which contained the 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 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 interpretations of the Health Insurance Portability and Accountability Act (HIPAA) being implemented by organizations and the challenges this variation would pose to nationwide electronic health information exchange (eHIE). Respondents noted that the HIPAA Privacy and Security Rules allow for 2 compliant hospitals to develop business practices entailing 2 different methods of protecting privacy and security and that this variation must be addressed if interoperable eHIE is to be achieved nationwide. Furthermore, the respondents noted that there would be complications both within and across states because of inconsistencies between state privacy laws and federal laws.

The purpose of this Privacy and Security Solutions for Interoperable Health Information Exchange project is to assess variations in organization-level business practices, policies, and state laws that affect eHIE 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. Because business practices are typically derived from business policies and law, uncovering the policy or legal driver on which the business practices are based is crucial to assessing whether a current practice will have any impact on electronic information exchange. If a current practice does have an impact, it is then crucial to determine whether it prevents or impedes the exchange, or whether it somehow makes the exchange more efficient. By developing a complete understanding of the rationale for a business practice, we can determine what elements should be retained as requirements for an electronic system of exchange and what elements of a given business practice can be streamlined or eliminated altogether. The final phase of the project will focus on developing detailed implementation plans.

The methodology developed for the project is based on 3 key assumptions. The first assumption is that, in order for eHIE to be trusted by the stakeholders actually using it, decisions about how to protect the privacy and security of health information should be made at the local community level. 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 that exists, 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 limited 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 in terms of purposes 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

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,
- hospitals,
- public health agencies,
- community clinics and health centers,
- laboratories,
- pharmacies,
- long-term care facilities and nursing homes,
- homecare and hospice,
- correctional facilities,
- professional associations and societies,
- medical and public health schools that undertake research,

- quality improvement organizations, and
- consumers or consumer organizations.

In the sections that follow, we summarize the various methods used by the state teams to organize their respective leadership teams and work groups, the methods used to engage stakeholders in the process, and the methods each state and territory followed to conduct the interim assessment of variation. Further, we summarize the state teams' findings by the 11 purposes for exchange and within domain wherever possible. Finally, we summarize 10 crosscutting issues raised by the state teams in the interim assessment of variation.

The methodology sections of the 34 interim reports focused primarily on narrating the activities that their working groups engaged in to obtain a comprehensive set of business practices from the stakeholder community. State teams provided varying degrees of detail when they described the composition and subject matter expertise of their Variations Work Groups (VWG) and Legal Work Groups (LWG). Because this report focused on the assessment of variations, none of the states discussed its Solutions Working Groups (SWG) or Implementation Planning Work Groups (IPWG).

It is important to note that there are limitations to what can be addressed in this report. This work represents a summary of work conducted by project teams in 34 of the 56 states and U.S. territories and therefore represents a "snapshot" of the current landscape in the 33 states and one territory that form HISPC, although many of the issues will cut across the entire nation. In addition, not much electronic exchange of health information is currently under way, and in many states these discussions are theoretical at best as states struggle to understand the issues involved.

1.1 Steering Committee Composition

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 had at least one member that represented the governor's office—either a senior policy advisor, cabinet member, or, in at least one state, 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. Most states that provided details about their steering committee membership notably included members from private or public task forces focused on improving eHIE; also included were directors of information technology services across the spectrum of state and private health care systems, including many chief information and security officers.

The breadth of stakeholder representation on the steering committee varied across the 34 state project teams. Although not many states provided the specific number of people on

their steering committees, where numbers were provided steering committees were generally smaller in number than the other working groups and less representative of the broader stakeholder community from which they drew. Some states with large American Indian populations included tribal representatives across all the working groups and not only in the steering committee. The state teams specifically had consumer group representation on their steering committees and in their working groups, including members of consumer advocacy organizations, as well as individual, unaffiliated consumers. As the project work evolves, state teams continue to work to ensure that they include consumer and patient input.

1.2 VWG and LWG Membership

Most of the state teams included details about the size and general composition of their VWGs and LWGs. As a whole, states attended to the need for breadth of stakeholder representation on the VWG. Some states decided to increase the size of their VWG to provide sufficient breadth in the group itself, while other states preferred to have a smaller VWG that gathered required information from the broader stakeholder community to achieve appropriate representation across that community. Of the 19 states that reported the size of their VWG, 5 states had more than 30 members, while the remaining states reported sizes between 12 and 20 members.

Although the states' working groups were not fully representative of the entire stakeholder community as described in the contract, states explicitly described the processes they used to engage those stakeholder groups not represented. All but a few of the state teams provided information about their VWG and LWG subject matter expertise as related to their particular stakeholder community. The few state teams that did not provide these details did describe the processes their work groups undertook to engage a wide variety of stakeholders to gather business practices. A few state teams explained in detail activities their VWG members engaged in to ensure a broader range of stakeholder involvement in gathering business practices.

LWG sizes were smaller across the board, ranging from 8 members to as many as 22 for the 13 state teams that included this information in their report. All but 9 state teams included some information about their LWG members' subject area expertise, and most of the LWG members' expertise was in private or public health care–sector legal affairs.

1.3 Outreach to Stakeholders

A leading researcher in the concept of the stakeholder, R. Edward Freeman, defines the *stakeholder* as an individual, or group, that has some share or interest in the functioning of the business system (1984).[2] Freeman explains that the term *stakeholder* is preferred over

[2] R. Edward Freeman. *Strategic Management: A Stakeholder Approach*. Boston: Pitman Publishing Company; 1984.

terms such as *constituents* or *influencers* because it connotes a level of accountability to the stakeholder by the business entity or initiative. The stakeholder can be as dynamic as the business system: depending on the issue, the stakeholder's level of interest, influence, and perspective may change. Each state team was therefore asked to identify the appropriate stakeholders for its project. In deference to these facts, RTI provided state teams minimal direction for identifying the stakeholders, except to request that the greatest effort be made to identify and include as many stakeholders as possible (for the list of recommended stakeholders to include in state working groups, see Appendix A). It should be noted that not all state teams were able to provide the distinction between consumer advocacy groups and the unaffiliated consumer. This distinction will be clarified in the final report.

The first step in developing an effective outreach strategy for stakeholders was for the state teams to create as comprehensive a list of stakeholders as possible on the basis of the privacy and security domains. By developing an initial list, the states were able to "piggyback" on that list and add more stakeholders as needed. Another phenomenon of the concept of the stakeholder is that various program levels spur various stakeholders. For example, on the administrative or management level the stakeholders may be different from those who will interface with the project on the operations level. Most state teams were able to address these nuances as they worked with their stakeholder groups by soliciting information from the appropriate participant level within them.

All of the state teams relied on a top-down approach in their outreach strategies. Once they agreed on a stakeholder, the initial contact was at the highest level to solicit participation and input from the organization or entity. The thought was that, for the type of detail required, participants needed to understand that their leadership supported their participation. Either information was then sent to the initial contact person, or an in-person contact was made to introduce the project. During the initial contact the state teams also detailed the expectations for participating in the work groups.

Once the states were provided the scenarios, the state teams revisited the lists of stakeholders and began grouping the stakeholders into work groups. The stakeholder work groups reviewed and analyzed scenarios relevant to their roles and concerns. Although there were differences among the state teams in how the work groups were formed or how the data were collected, there were no differences in the level of effort expended to identify and reach stakeholders.

1.4 Outreach Methods

To enhance outreach, the state teams

- circulated documents to all active members of health organizations, most of whom work in medical records or a related area;

- reached out to stakeholder and professional associations, government agencies at all levels, and consumer groups;
- held regional meetings and broke work groups into sublevel work groups;
- highlighted the project on Web sites and in newsletters;
- identified individuals to participate in focus groups or on Listservs;
- capitalized on existing health information technology (HIT) collaborations and partnerships;
- sought stakeholder involvement through word-of-mouth invitations;
- through VWG members, recommended additional stakeholders who were invited to participate; and
- provided a public e-mail address so that interested persons could participate in the project.

1.5 List of Stakeholders

Following is a list of stakeholders reported to be engaged in the project across the 34 state teams:

- health care providers (including mental health and substance abuse treatment providers)
- hospital/clinic administrators (CEOs/directors, privacy officers, CIOs)
- pharmacists
- attorneys
- law enforcement information technology (IT) personnel
- insurance administrators
- homecare and hospice staff
- epidemiologists
- health information management professionals
- emergency medical services
- eHIE and regional health information organization (RHIO) board members
- correctional facilities
- state government (personal injury protection insurance, workers' compensation, disability insurance, Social Security)
- homecare and hospice facilities
- long-term care
- payers and plans
- physician groups—large and small

- professional organizations and societies
- consumer advocacy organizations
- policy makers
- HIT leaders
- unaffiliated consumers
- homeless shelters
- mental health and substance abuse associations
- clearinghouses
- trade associations
- academic institutions
- employers and unions
- vendors
- laboratories
- special interest groups

1.6 Approaches to Conducting the Work

1.6.1 Plan

In June and July 2006, RTI conducted a series of Web-based conference calls and in-person trainings to introduce the state project teams to the project tools that had been developed, including the 18 scenarios and the Agency for Healthcare Research and Quality (AHRQ) National Resource Center portal, and, on the basis of these tools, to suggest an approach to the work. This approach consisted of 4 main steps through the submission of the Interim Assessment of Variation (IAV) report. Although this process is delineated here as a sequence of separate steps, it is actually a dynamic and interactive iterative process; most state teams managed the process by having considerable overlap in the composition of their work groups.

Step 1

The VWG members were to review as many of the 18 health information exchange (HIE) scenarios as their knowledge and experience allowed and generate a core set of business practices and policies consistent with the stakeholder roles represented in the scenarios. VWG members could also at this stage begin to identify business practices for which policy decisions may be needed to transition from a paper-based system to eHIE. As part of this initial step, project teams were asked to categorize business practices as potential barriers to eHIE; as potential enablers of or aids to eHIE; or as having no impact on the flow of information, whether on paper or electronically.

In this scheme, the term *barrier* was initially defined as any business practice that impeded or blocked the electronic flow of information; it was intended to "flag" any business practice for which an understanding of the underlying rationale (ie, the policy or legal driver) would be required to guide decisions about whether the practice was necessary. If the practice was deemed necessary, this understanding would also guide reconciliation of the practice with the need to exchange the information electronically. Similarly, the category of *aid to eHIE* was to flag practices for review as potentially "good" practices that could be shared with other organizations and states.

The project team, the Technical Advisory Panel (TAP), and the state teams wrestled with the term *barrier* as applied to individual practices because of its negative connotations. The project focus is on the *variation* in practice, policy, and law that poses a barrier to interoperable eHIE, not on individual practices that may or may not be barriers to interoperable eHIE. The definition was refined in an attempt to remove the value-judgment and was then presented as "a practice, policy, or law that impedes, prohibits, or imposes conditions on health information exchange." States were asked not to make a decision at this point in the process about whether a practice categorized as a barrier was "an appropriate protection" or an overly restrictive practice that could be modified; instead, they were asked to flag practices for further scrutiny.

Although many state teams followed this approach, a number of state teams took the position that under this definition informed consent would be a barrier and, even though it could be called "an appropriate protection" or a "good" barrier, the label *barrier* would nonetheless be a bad fit in this context. The project team ultimately decided that states could use their own method of flagging the business practices for further evaluation and consideration by their work groups. There are many references to *barriers* throughout this report; these references derive from the text provided by the state reports and the definition provided here.

Step 2

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

On the basis of the American Health Information Management Association's (AHIMA) experience during development and pilot testing of the scenarios, RTI suggested that this step might be most effectively accomplished through a series of facilitated meetings, but RTI recognized that such meetings would not be feasible for all state teams. AHIMA and RTI prepared a guide to facilitating these meetings, which was included in the *Manual of Operations*. To ensure efficiency during use of the facilitated-meeting model, meetings were organized around subsets of the 18 scenarios, and the relevant stakeholders were invited to

attend each meeting. State teams submitted plans describing their preferred methods for organizing the stakeholder groups.

Step 3

The VWG reviewed the full set of collected business practices to ensure that the data were complete and sufficiently detailed for use by the LWG; in addition, the VWG was charged with identifying those business practices for which policy decisions might be needed.

Step 4

The collected business practices that were flagged by the VWG were reviewed by the LWG to identify and capture any legal drivers that might be relevant.

Each state team was granted considerable latitude to determine, given its own circumstances, the specific approach that would work best for it. In particular, state teams determined the best methods for engaging a broad group of stakeholders in the review of scenarios.

1.6.2 Outcomes

The VWGs' task was to review the scenarios, generate a core set of business practices, and begin to identify challenges to interoperable eHIE. VWGs achieved broad coverage of stakeholder groups and state regions. In order to increase coverage of stakeholder perspectives, some states expanded the VWG to include additional individuals from participating organizations.

The function of the VWG varied across teams. Most collected a core set of business practices as suggested. Others generated the initial set of business practices in meetings that combined the VWG with the broader group of stakeholders. A few asked stakeholders to generate the initial set of business practices, and then the VWG reviewed and filled gaps. Before collecting business practices, some VWGs identified interoperability challenges based on their perceptions of the scenarios. Shortly after receiving the scenarios, one state team generated a core set of questions or topic areas for each scenario to guide stakeholder discussion. These questions were shared with RTI, AHRQ, the Office of the National Coordinator for Health Information Technology (ONC), and selected TAP members for review and comment. It was then distributed to all project teams in the form of a scenario guide.

The practices collected were shared with a broader group of stakeholders to validate that as a set they were reasonably complete and to fill gaps as necessary. All teams engaged the broader stakeholder community. Participation numbers ranged from 30 to approximately 300 stakeholders. Facilitated meetings were used by most teams, but additional techniques were usually employed to collect supplementary data from stakeholders. Additional

stakeholder input was collected by telephone and in-person interviews, conference calls, e-mail, submissions to Web sites, and submittal of completed worksheets.

Stakeholders were usually asked to review and vet the core set of business practices generated by the VWG. A number of reports note that they also sent background materials, scenarios, and the core set of business practices to stakeholders in advance of the meeting.

A few teams noted that they added scenarios or modified the provided scenarios to adapt them to particular circumstances in their respective states or territory.

Most project teams arranged meetings organized by subsets of scenarios that required input from a common set of stakeholder groups. Usually 2 to 5 scenarios were reviewed per meeting. This approach also allowed teams to limit participation to a manageable size to encourage active participation. Most teams reported that 2 to 3 members of the core team attended the stakeholder meetings to provide background, facilitate, and take notes.

Six teams reported that they encountered concerns about confidentiality and anonymity when they solicited input from stakeholders. Three teams reported that they developed a consent agreement to address these concerns. One state reported that stakeholder participation was limited because some recruits were prohibited from sharing their practices, citing proprietary business practice information. A few states reported participants who were unwilling to share business practices despite assurances of confidentiality and anonymous reporting.

Some teams noted an inability to engage, in this phase of the work, particular stakeholder groups, such as consumers, law enforcement, and federal health facilities. These project teams reported continuing efforts to engage these stakeholder groups so they would be able to include their input in the final Assessment of Variation and Analysis of Solutions reports.

All teams made a conscious effort to assess the completeness of the coverage they had achieved between their VWG membership and the stakeholders they were able to engage. They solicited additional input through targeted recruitment as necessary to fill gaps. Many teams reported that they cycled back to collect additional information as necessary to ensure that their information was sufficiently specific and complete. Many teams also reported that they distributed the larger, final set of business practices to the entire group of participants as a final quality control check on the accuracy of note-taking and data entry.

All state teams mapped legal drivers to business practices, although in some instances the work was not finished at the time of report submission. Rather than wait to receive business practice data, at least 12 LWGs chose, on the basis of their review of each scenario, to compile compendiums of relevant law. This method proved efficient, allowing LWGs to map legal drivers to business practices as soon as business practices became available.

1.6.3 Representativeness of Business Practices

In designing the process for assessing variation in business practices related to eHIEs, the project team faced the major challenge of ensuring that the business practices identified by the states were comprehensive and represented the broad range of entities that might participate in such eHIEs. There are many stakeholder groups and often many constituents within each stakeholder group (eg, providers). Seventeen groups were named in the request for proposals sent to each of the states and territories, with the option of identifying additional stakeholders (for a complete list of stakeholders, see Appendix A). Statistical sampling methods would have provided a quantitative approach to estimating the representativeness of each stakeholder sample; however, because of project schedule and budget constraints, developing statistical designs and sampling frames for each of these groups was not feasible.

The approaches to conducting the work address representativeness in several ways. First, the scenarios were developed to represent a wide range of stakeholders, as well as an array of contexts for HIE. Second, each participating state and territory was specifically required to demonstrate the capability to ensure participation by a wide 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 also covered during the training of each of the state teams to ensure that, as a practical matter, states would have the appropriate groups participating. Fourth, the design of the assessment process relies on a recursive approach, one in which practices identified by the VWG are vetted with larger groups of stakeholders at several points in the assessment process to identify and fill gaps. Finally, we should emphasize that this process is ongoing. The results of the state teams' interim reports have been reviewed with this issue in mind, and feedback will be provided to state teams to incorporate into the final assessment of variation.

2. SUMMARY OF DISCUSSIONS GENERATED BY THE HEALTH INFORMATION EXCHANGE SCENARIOS

This section summarizes the relevant findings generated by the work group discussions held in each state to generate the universe of business practices necessary to conduct the interim assessment of variation. The work group discussions were based on 18 scenarios that represented 11 different purposes or types of health information exchange (HIE) involving a broad range of stakeholders. The American Health Information Management Association (AHIMA) was subcontracted by RTI to develop and test a set of 18 scenarios that would provide 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 B). 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 form the basis for the assessment of variation in organization-level business practices.

Purposes for HIE

- Treatment
- Payment
- Regional HIE (RHIO)
- Research
- Law enforcement
- Prescription drug use/benefit
- Operations
- Bioterrorism
- Employee health
- Public health
- State government oversight

This section is organized by the 11 purposes for exchange, and it summarizes the following for each subsection: (1) the range of stakeholders that states or territories engaged in each of the discussions on the relevant scenarios, (2) the key domain areas affected, and (3) the primary issues identified as impacting interoperability.

2.1 Treatment (Scenarios 1–4)

1. Patient Care Scenario A

Patient X presents to emergency room of General Hospital in State A. She has been in a serious car accident. The patient is an 89-year-old widow who appears very confused. Law enforcement personnel in the emergency room investigating the accident indicate that the patient was driving. There are questions concerning her possible impairment due to medications. Her adult daughter informed the ER staff that her mother has recently undergone treatment at a hospital in a neighboring state and has a prescription for an antipsychotic drug. The emergency room physician determines there is a need to obtain information about Patient X's prior diagnosis and treatment during the previous inpatient stay.

Potential areas for discussion of BUSINESS PRACTICES based on this scenario:

1. Determining status of the patient and chain of responsibility.
2. Practice and policy for obtaining information sufficient for treatment.
3. Practice and policy for handling mental health information.
4. Practice and policy for securing the data exchange mechanism.
5. Practice and policy related to authentication of requesting facility by the releasing facility.
6. Practice and policy related to patient authorization for the release of information.

2. Patient Care Scenario B

An inpatient specialty substance abuse treatment facility intends to refer client X to a primary care facility for a suspected medical problem. The 2 organizations do not have a previous relationship. The client has a long history of using various drugs and alcohol that is relevant for medical diagnosis. The primary care provider has requested that the substance abuse information be sent by the treatment facility. The primary care provider intends to refer the patient to a specialist and plans to send all of the patient's medical information, including the substance abuse information that was received from the substance abuse treatment facility, to the specialist.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. How does the releasing organization obtain authorization from the patient to allow release of medical records?
2. What is the process for handling substance abuse medical records data?
3. How does the releasing organization authenticate the health care provider requesting the information?
4. How is the data exchange secured?

3. Patient Care Scenario C

At 5:30 p.m., Dr. X, a psychiatrist, arrives at the skilled nursing facility to evaluate his patient, recently discharged from the hospital psychiatric unit to the skilled nursing facility. The hospital and skilled nursing facility are separate entities and do not share electronic record systems. At the time of the patient's transfer, the discharge summary and other pertinent records and forms were electronically transmitted to the skilled nursing home.

When Dr. X enters the facility, he seeks assistance locating his patient, gaining entrance to the locked psychiatric unit, and accessing the patient's electronic health record to review the discharge summary, I&O, MAR, and progress notes. Dr. X was able to enter the unit by showing a picture identification badge, but was not able to access the EHR. As it is Dr. X's first visit, he has no log-in or password to use their system.

Dr. X completes his visit and prepares to complete his documentation for the nursing home. Unable to access the skilled nursing facility EHR, Dr. X dictates his initial assessment via telephone to his outsourced, offshore transcription service. The assessment is transcribed and posted to a secure Web portal.

The next morning, from his home computer, Dr. X checks his e-mail and receives notification that the assessment is available. Dr. X logs into his office Web portal, reviews the assessment, and applies his electronic signature.

Later that day, Dr. X's office manager downloads this assessment from the Web portal, saves the document in the patient's record in his office, and forwards the now encrypted document to the long-term care facility via e-mail.

The skilled nursing facility notifies Dr. X's office that they are unable to open the encrypted document because they do not have the encryption key.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Agreements for data sharing—business associate agreements.
2. Setting out access and role management policies and practices for temporary or new access.
3. Determining appropriate access to mental health records.
4. Securing unstructured, possibly nonelectronic patient data.
5. Reliability of other entity security and privacy infrastructure.

4. Patient Care Scenario D

Patient X is HIV positive and is having a complete physical and an outpatient mammogram done in the Women's Imaging Center of General Hospital in State A. She had her last physical and mammogram in an outpatient clinic in a neighboring state. Her physician in State A is requesting a copy of her complete records and the radiologist at General Hospital would like to review the digital images of the mammogram performed at the outpatient clinic in State B for comparison purposes. She also is having a test for the *BrCa* gene and is requesting the genetic test results of her deceased aunt who had a history of breast cancer.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Authenticating entities and individuals.
2. Determining processes and laws for release of genetic and HIV information.

2.1.1 Stakeholders

For Scenarios 1 through 4, RTI suggested that the stakeholder groups engaged in the review of the scenarios and asked to describe business practices include hospitals, substance abuse treatment facilities, physicians, public health agencies, patient-consumers, and community clinics and health centers.

All stakeholder groups were engaged in the review of Scenarios 1 through 4. The frequency with which each of the stakeholder groups was engaged in the review and discussion is shown in Table 2-1. The most frequently engaged stakeholder groups were hospitals, engaged by all the state teams; clinicians, engaged by 88%; physician groups, engaged by 85%; long-term care facilities, engaged by 59%; community clinics, engaged by 50%; and consumers and consumer groups, engaged by 50%.

2.1.2 Domains

Table 2-2 shows the domains of privacy and security affected by business practices reported for each state team.

There was considerably little variation regarding domains examined across the state teams, with more than half of the state teams addressing 8 or all 9 of the domains. The top 4 domain areas included were as follows:

- Domain 2—Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information (eHIE; 100%);
- Domain 9—Information use and disclosure policies that arise as health care entities share clinical health information electronically (97%);
- Domain 1—User and entity authentication to verify that a person or entity seeking access to electronic personal health information is who they claim to be (91%); and
- Domain 4—Information transmission security or exchange protocols (ie, encryption) for information that is being exchanged over an electronic communications network.

Table 2-1. Stakeholder Groups Engaged in Scenario 1–4 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenarios 1–4 (N = 34)
Hospital personnel/emergency room staff	34 (100%)
Clinicians	30 (88%)
Physician groups	29 (85%)
Long-term care facilities	20 (59%)
Consumers/consumer organizations	17 (50%)
Community clinics and health centers	17 (50%)
State government	10 (29%)
Behavioral health	10 (29%)
Nursing homes	9 (26%)
Public health agencies	7 (21%)
Correctional facilities personnel	6 (18%)
Homecare and hospice	6 (18%)
Pharmaceutical companies	6 (18 %)
Professional associations	6 (18%)
Schools	6 (18%)
Federal health facilities	5 (15%)
Health information management/transcription	5 (15%)
Quality improvement organizations	5 (15%)
Attorneys	5 (15%)
Laboratories	5 (15%)

2.1.3 Critical Observations

Critical observations related to the treatment scenarios were fairly uniform, although there were numerous variations described in the handling of health information. In many states, paper-based records are still the norm, and patient information is exchanged informally, most often verbally and by fax. In this context, privacy and security policies are 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. For organizations that used an electronic health record (EHR), significantly more procedures were in place to protect patient information, including training, signed confidentiality statements, and access controls. In nearly all states, additional protections and restrictions were placed on special categories of sensitive information, including drug and alcohol diagnoses and treatment, mental health information, HIV/AIDS diagnoses, and genetic information.

Table 2-2. Nine Privacy and Security Domains Affected by Business Practices Associated With Scenarios 1–4 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X	X	X	X	X	X	X	X
Arizona	X	X	X	X		X	X	X	X
Arkansas	X	X	X	X			X	X	X
California	X	X				X		X	X
Colorado	X	X	X	X	X	X	X		X
Connecticut	X	X	X	X	X	X	X	X	X
Florida	X	X	X	X			X	X	X
Illinois	X	X	X	X	X	X	X		X
Indiana		X		X	X	X			X
Iowa	X	X	X	X	X	X	X	X	X
Kansas	X	X	X	X	X	X	X	X	X
Kentucky	X	X		X		X	X	X	X
Louisiana	X	X		X	X	X	X	X	X
Maine	X	X	X	X	X	X	X	X	X
Massachusetts	X	X	X	X	X		X	X	X
Michigan	X	X	X	X	X	X	X	X	X
Minnesota	X	X	X	X	X	X	X	X	X
Mississippi	X	X	X	X					X
New Hampshire		X							X
New Jersey	X	X		X			X	X	X
New Mexico	X	X	X	X	X	X	X	X	X
New York	X	X	X	X	X		X	X	X
North Carolina	X	X	X	X	X	X	X	X	X
Ohio	X	X							
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon	X	X	X	X			X	X	X
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island		X		X	X			X	X
Utah	X	X		X	X		X	X	X
Vermont	X	X	X	X	X	X	X		X
Washington	X	X	X	X	X	X	X	X	X
West Virginia	X	X	X	X	X	X	X	X	X
Wisconsin	X	X	X	X	X	X	X	X	X
Wyoming	X	X	X	X					X
Total	31 (91%)	34 (100%)	25 (74%)	31 (91%)	23 (68%)	22 (65%)	27 (79%)	26 (76%)	33 (97%)

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An empty cell indicates that no business practice was identified in association with that domain.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires that providers use and release only the "minimum necessary" personal health care information to achieve the intended purpose. The state teams reported widespread variation, however, in how the *minimum necessary* standard is understood and applied. The state teams reported that there is no clear definition of what *minimum necessary* should consist of in any given situation. The level of information provided to satisfy this standard varies not only from organization to organization, but also between people within the same organization. Although obtaining patient consent is a widespread practice across providers in most states, the policies and procedures for obtaining consent vary considerably.

Interstate exchange of health information and the requesting of health information for out-of-state patients constitute an area not well understood by many of the stakeholders. The state teams identified broad variation in practices followed to exchange protected health information (PHI), including variation in data definitions, transmission protocols, and authentication 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. In addition, both paper-based and electronic information systems employ a wide range of incompatible practices that can lead to misinterpretation by users outside of the originating systems.

2.2 Payment (Scenario 5)

5. Payment Scenario

X Health Payer (third party, disability insurance, employee assistance programs) provides health insurance coverage to many subscribers in the region the health care provider serves. As part of the insurance coverage, it is necessary for the health plan case managers to approve/authorize all inpatient encounters. This requires access to the patient health information (eg, emergency department records, clinic notes).

The health care provider has recently implemented an electronic health record (EHR) system. All patient information is now maintained in the EHR and is accessible to users who have been granted access through an approval process. Access to the EHR has been restricted to the health care provider's workforce members and medical staff members and their office staff.

X Health Payer is requesting access to the EHR for their accredited case management staff to approve/authorize inpatient encounters.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Get patient authorization to allow payer access.
2. Facility needs to determine the minimum necessary and limit to pertinent time frame.
3. If allowed, access and role management are issues.
4. Determine method for enabling secure remote access if allowed.

2.2.1 Stakeholders

Overall, the state teams included a wide variety of stakeholders in discussions for Scenario 5. While some states were able to draw from a large pool of stakeholders, other states were able to include only a few stakeholders for this scenario. Although stakeholder variation among states was great, 2 of the stakeholder groups that would be most directly affected by this scenario were well represented, with 30 of the 34 state teams including a payer stakeholder in discussions and with 28 of the 34 including hospital personnel (Table 2-3). In contrast, consumers, another stakeholder group highly likely to be affected by this scenario, were represented in only 15 states. Other common stakeholder groups, each represented in 10 to 12 states, were clinicians, physician groups, and state government.

Table 2-3. Stakeholder Groups Engaged in Scenario 5 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenario 5 (N = 34)
Payers/insurance	30 (88%)
Hospital personnel/emergency room staff	28 (82%)
Consumers/consumer organizations	15 (44%)
Physician groups	12 (35%)
Clinicians	11 (32%)
State government	10 (29%)
Homecare and hospice	9 (26%)
Community clinics and health centers	8 (24%)
Federal health facilities	6 (18%)
Long-term care facilities/nursing homes	6 (18%)
Public health agencies	6 (18%)
Pharmaceutical companies	4 (12%)
Professional associations	4 (12%)
Laboratories	2 (6%)
Quality improvement organizations	2 (6%)
Regional health information organization (RHIO) representatives	2 (6%)
Information security	2 (6%)
Medical and public health schools that undertake research	1 (3%)
Correctional facilities personnel	1 (3%)
Substance abuse centers	1 (3%)

2.2.2 Domains

There was wide variation in how the state teams viewed Scenario 5, some feeling that all 9 domains were relevant to this scenario and others feeling that this scenario involved only 1

or 2 domains. Despite this variation among the state teams, 30 of the 34 of them stated that Domain 2—"Information authorization and access control to allow access only to people or software programs that have been granted access rights to electronic personal health information"—was related to this scenario.

To ensure that users have access only to appropriate information, state teams are using procedures such as log-in names and passwords to help identify the user and role-based access. Some state teams found that nonexistent access control procedures in partner organizations were a barrier to eHIE. Additionally, some state teams found that hospital systems and payers do not use a standardized protocol for role-based access beyond their own facility and therefore cannot distinguish whether users from other facilities have permission to access treatment data, sensitive data, or more general data. A related issue was the lack of access to organizations' electronic systems by third-party administrators. Most organizations do not allow any kind of remote access to their systems by outside parties.

Twenty-six of the 34 states listed Domain 9—"Information use and disclosure policies that arise as health care entities share clinical information electronically"—as valid for this scenario (Table 2-4). State teams found that many health care providers have no written policies to address this issue. There was agreement that patients authorize release for payment purposes (not for access to medical records), that patient consent is required by the payer before any disclosure, and that payers should have access to only *minimum necessary* patient information. There was also agreement that no HIPAA issues were associated with this scenario beyond the definition of *minimum necessary* because PHI may be used for treatment, payment, and health care operations (TPO) without written consent from the patient.

The third most common domain cited by the state teams for the payer scenario was 1—"User and entity authentication is used to verify that a person or entity seeking access to electronic personal health information is who they claim to be." Of the 34 states, 21 felt this domain was relevant to Scenario 5. Currently, most providers ask for a written request from the insurance company or use a call-back procedure to authenticate the identity of the requestor if they are not in regular contact with the person calling.

2.2.3 Critical Observations

A common theme among the states is the issue of 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 EHR, and generally access by nonhospital personnel is restricted and often limited to hard copies of medical records. Although access to health information by payers is not permitted, HIEs with payers are completed by means of providers' requests for data from payers. There is confusion among the states and providers as to what amount of information regarding the patient meets the *minimum necessary*

Table 2-4. Nine Privacy and Security Domains Affected by Business Practices Associated With Scenario 5 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X	X	X	X	X	X	X	X
Arizona	X	X	X	X		X	X	X	X
Arkansas	X	X	X	X	X				X
California		X				X	X		X
Colorado		X					X		X
Connecticut	X	X	X	X	X	X	X	X	X
Florida		X						X	X
Illinois	X	X							
Indiana		X			X				
Iowa		X	X	X	X	X	X		X
Kansas	X	X	X	X	X	X	X	X	X
Kentucky	X	X		X	X	X	X	X	X
Louisiana	X	X	X			X	X		
Maine	X	X				X			
Massachusetts								X	X
Michigan	X	X	X	X	X	X			X
Minnesota	X	X			X	X	X	X	X
Mississippi		X		X		X			X
New Hampshire									X
New Jersey	X	X		X				X	
New Mexico		X						X	
New York	X	X					X		
North Carolina	X	X	X	X	X	X	X	X	X
Ohio		X							X
Oklahoma	X	X	X	X	X		X	X	X
Oregon	X	X				X	X		X
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island		X							X
Utah		X							X
Vermont		X		X		X			X
Washington	X	X	X	X	X	X	X		X
West Virginia	X		X	X				X	
Wisconsin	X	X	X	X	X			X	X
Wyoming	X								X
Total	21 (62%)	30 (88%)	14 (41%)	17 (50%)	14 (41%)	17 (50%)	16 (47%)	15 (44%)	26 (76%)

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An empty cell indicates that no business practice was identified in association with that domain.

requirement of HIPAA. The issue of granting access in a HIPAA-compliant manner was a concern commonly reported by the state teams.

Patient consent was another issue discussed in many state team reports. Most states agreed that when a patient signs a release form it is for information necessary for payment (*minimum necessary*), not for the payer's access to his or her entire medical record. The state team reports indicate wide variation among organizations in deciding when patient consent is required; how the consent is obtained and documented; and how patient consent is communicated to health care organizations, payers, and other outside entities.

In their discussions of the domains of authorization and access controls, the state teams reported that currently providers use means such as log-in names and passwords to limit access to electronic information. Additionally, role-based access helps ensure users have access only to the information that they need and 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. Common criteria must be established for this security measure to be effective in controlling access by outside parties. Additionally, time and effort must be spent in developing an electronic system that will restrict access where necessary instead of allowing complete EHR access to all users. Many state teams found that providers were currently unwilling to spend the time and money necessary to make these provisions.

Another common theme is the issue of trust. Consumers have expressed a general concern about who can access their health information and for what purposes. Patients particularly do not trust that payers and employers will refrain from using their EHR in an unethical way if they have access to it. In addition, some patients are concerned that the release of records containing information related to drug abuse, mental health, alcoholism, or HIV/AIDS may cause substantive harm to individuals and families.

There also seems to be a sense of distrust among providers regarding EHRs. They are concerned the information will be used against them in setting rates. Providers do not trust that others who participate in eHIE will protect health information to the same degree that they themselves do, thereby exposing them to potential liability.

This lack of trust might lead to organizations' and individuals' refusals to participate in an eHIE system if it becomes available. Substantively addressing these concerns, as well as educating both the public and providers about security policies and measures, will be crucial to the adoption of eHIE.

2.3 RHIO (Scenario 6)

6. RHIO Scenario

The RHIO in your region wants to access patient-identifiable data from all participating organizations (and their patients) to monitor the incidence and management of diabetic patients. The RHIO also intends to monitor participating providers to rank them for the provision of preventive services to their diabetic patients.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Decision to utilize medical record data to monitor disease management.
2. Authorization from patients to allow RHIO to monitor their PHI for disease management.
3. Determine mode of transferring information and type of information, ie, identifiable or de-identified information to the RHIO.

2.3.1 Stakeholders

Scenario 6 was included to provide a context for discussions in states that do have some eHIE activity. No definition of the term *RHIO* was provided, leaving it open to the state teams to define as needed. A total of 8 state teams offered no responses for this scenario because their states currently have no eHIEs in operation. As shown in Table 2-5, the 26 state teams that did respond to this scenario included a wide variety of stakeholders in discussions. Because of this diversity, the most common stakeholder, hospitals, appeared in only 13 of the 26 responding states. Other common stakeholders were physicians groups and payers, in 11 and 10 states, respectively.

2.3.2 Domains

One state team responded to this scenario but did not list any domains related to it, leaving a total of 25 states that selected domains. As with other scenarios, opinions varied widely among the states as to which domains were relevant to this scenario. Limited stakeholder response to this scenario in some states may have had an effect on the domains selected.

Of the 25 states that selected domains for this scenario, 21 listed Domain 9—"Information use and disclosure policies that arise as health care entities share clinical information electronically"—as being relevant to this scenario (Table 2-6). States agreed that sharing de-identified data with the RHIO would not necessarily be a problem, but patient or institutional review board (IRB) approval would be necessary to send identifiable data. Additionally, hospitals would require some kind of "business associate" agreement (BAA) or confidentiality agreement with the RHIO before sending data.

Table 2-5. Stakeholder Groups Engaged in Scenario 6 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenario 6 (N = 26)[a]
Hospitals	13 (50%)
Physician groups	11 (42%)
Payers	10 (38%)
Clinicians	9 (35%)
Community clinics and health centers	9 (35%)
Consumers/consumer organizations	7 (27%)
Public health agencies	7 (27%)
Homecare and hospice	7 (27%)
RHIO representatives	7 (27%)
Federal health facilities	6 (23%)
Laboratories	6 (23%)
Pharmaceutical companies	6 (23%)
Long-term care facilities/nursing homes	6 (23%)
Professional associations	6 (23%)
State government	5 (19%)
Quality improvement organizations	4 (15%)
Correctional facilities personnel	3 (12%)
Information security	3 (12%)
Medical and public health schools that undertake research	2 (8%)
Attorneys	2 (8%)
Law enforcement	1 (4%)
Mental health	1 (4%)
Data vendors	1 (4%)
Advocacy groups	1 (4%)

[a] Eight of the 34 states did not respond to the RHIO scenario.

Domain 2—"Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information"—was selected by 16 states as being relevant to this scenario; 16 states also selected as relevant Domain 4—"Information transmission security or exchange protocols for information that is being exchanged over an electronic communications network." States indicated that proper encryption methods, or use of a secure file transfer protocol (FTP), were needed to transmit data to the RHIO. Additionally, access to PHI transmitted through a RHIO is usually role-based, with permissions set according to an individual's affiliation with one of the connecting institutions.

Table 2-6. Nine Privacy and Security Domains Affected by Business Practices Associated With Scenario 6 (N = 34)[a]

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X		X	X					X
Arizona									
Arkansas									
California		X							X
Colorado		X	X	X				X	X
Connecticut	X	X	X	X	X	X	X	X	X
Florida								X	X
Illinois	X	X							
Indiana				X					X
Iowa		X	X	X			X	X	
Kansas	X	X	X	X	X	X	X	X	X
Kentucky	X	X		X	X	X	X	X	X
Louisiana	X	X		X			X		X
Maine				X					X
Massachusetts				X				X	X
Michigan	X	X							X
Minnesota	X	X	X	X	X	X	X	X	X
Mississippi				X					X
New Hampshire									
New Jersey									
New Mexico		X						X	
New York		X							X
North Carolina	X	X	X	X	X	X	X	X	X
Ohio									X
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon									
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island									
Utah									
Vermont									
Washington				X			X		X
West Virginia			X					X	X
Wisconsin									
Wyoming		X							
Total	11 (44%)	16 (64%)	10 (42%)	16 (64%)	7 (28%)	7 (28%)	10 (42%)	13 (52%)	21 (84%)

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An empty cell indicates that no business practice was identified in association with that domain.

[a]In addition to the 8 state teams' not responding to this scenario, one state team out of the 34 did not list any domains associated with this scenario.

2.3.3 Critical Observations

There is uncertainty in some states about the functions of an eHIE, specifically as it relates to data collection, analysis, and disease management. Several state teams were unsure of an eHIE's legal status in their state, and opinions differed as to whether an eHIE was a HIPAA-covered entity. Although the scenario indicated that the RHIO wanted to "access patient-identifiable data," most states responded that they would share only de-identified data with the RHIO. Patient consent would be required for the RHIO to receive patient-identifiable data. Several state teams mentioned that there were no current state laws prohibiting the use of medical information to monitor disease management if the data are de-identified and the patients are not contacted.

State teams agreed that, if information is to be exchanged, whether it is patient-identifying or whether it is de-identified, security is of the utmost importance. To remain compliant with HIPAA, state teams indicated that they would need to have a BAA with the RHIO before sending data. Data files either would have to be sent encrypted or would have to be uploaded to a secure Web site. The RHIO itself would have to have security measures such as password-protected computers, credentialing and authentication of users, and role-based access in place to keep any data it received secure.

Some state teams were uncomfortable with the idea of the RHIO's ranking participating providers. Some specific concerns included the following: the ranking of providers would likely jeopardize the neutrality of a RHIO; a RHIO must have broad participation, and providers might not want to participate if they know they are being ranked; providers who participate may be unfairly compensated because of referrals associated with their ranking; and consumers may mistakenly assume that a nonparticipating provider is somehow better than a ranked, participating provider.

Another common theme among the state teams regarding RHIOs was the different levels of technical capabilities of organizations (large versus small, urban versus rural), a difference that amounts to a "capacity gap" for some entities that may participate in those RHIOs.

2.4 Research Data Use Scenario (Scenario 7)

7. Research Data Use Scenario

A research project on children younger than age 13 is being conducted in a double-blind study for a new drug for ADD/ADHD. The research is being sponsored by a major drug manufacturer conducting a double-blind study approved by the medical center's IRB, where the research investigators are located. The data being collected are all electronic, and all responses from the subjects are completed electronically on the same centralized and shared database file.

The principal investigator was asked by one of the investigators if they could use the raw data to extend the tracking of the patients over an additional 6 months or use the raw data collected for a white paper that is not part of the research protocols final document for his postdoctoral fellow program.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. IRB approval of any significant changes to the research protocol.
2. Research subjects have signed consents and authorization to participate in the research effort.

2.4.1 Stakeholders

All the state teams included representatives from university research groups, health care providers representing both hospitals and clinics, members of IRBs, and consumer advocates in discussion of Scenario 7. State teams paid special attention to including stakeholders from medical schools and their hospitals' clinical research staff members. Some state teams specifically mentioned including correctional facilities officials. One state team noted that its stakeholders for this scenario included participants in clinical trials, as well as a grants administrator familiar with human subject research guidelines. A few state teams included stakeholders from hospice, long-term care, and nursing home facilities (Table 2-7).

2.4.2 Domains

Domains 9 and 2 emerged as those most often cited by the state teams (Table 2-8). Eighty-eight percent of the state teams identified Domain 9—"Information use and disclosure policies that arise as health care entities share clinical information electronically"—as the most relevant to the scenario's topic, and these state teams reported significant disagreement among their stakeholders regarding the limitations of the permitted scope of research under the original IRB approval. For Domain 2, more than half the state teams focused on its requirement that the patient, or consumer, provide authorization for the researcher to access that patient's data. The other 7 domains were nearly evenly selected by a third or so of the state teams.

The other 7 domains often came into play with regard to proper data storage and data-sharing activities. Stakeholders discussed de-identification procedures, data encryption requirements, and the purpose scope of the requested research protocol as related to

Table 2-7. Stakeholder Groups Engaged in Scenario 7 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenario 7 (N = 34)
Medical and public health schools that undertake research	20 (59%)
Hospital personnel/emergency room staff	17 (50%)
Clinicians	15 (44%)
Consumers/consumer organizations	13 (38%)
Public health agencies	11 (32%)
IRB members	9 (26%)
Physicians	9 (26%)
State government	8 (24%)
Federal health facilities	4 (12%)
Homecare and hospice	4 (12%)
Community clinics and health centers	3 (9%)
Pharmacies	3 (9%)
Professional associations	3 (9%)
Laboratories	3 (9%)
Payers	3 (9%)
Long-term care facilities/nursing homes	3 (9%)
Information security	1 (3%)
Quality improvement organizations	1 (3%)
Correctional facilities personnel	1 (3%)
Attorneys	1 (3%)

the other domains associated with user and entity authentication, information authorization and access controls, information transmission security or exchange protocols, and administrative or physical security safeguards.

2.4.3 Critical Observations

State teams gave numerous reports of lively discussions about the specific requirements imposed on the Scenario 7 researcher by the IRB, and nearly all the stakeholders reported that the IRB approval process was the most significant discussion point for the provision of data in this scenario. State teams' critical observations regarding Scenario 7 echoed each other by noting that many of their stakeholders would always seek a new signed consent from the study participants or guardians: the original consent did not include consent for data to be used outside the approved IRB protocols, and it required time extensions for data-sharing provisions.

Table 2-8. Nine Privacy and Security Domains Affected by Business Practices Associated With Scenario 7 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X	X		X		X		
Arizona	X	X		X	X				X
Arkansas		X		X		X	X	X	X
California						X			X
Colorado		X					X		X
Connecticut	X	X	X	X	X	X	X		
Florida		X						X	X
Illinois									X
Indiana		X							X
Iowa		X					X		X
Kansas	X	X		X	X	X	X	X	X
Kentucky						X	X		X
Louisiana		X	X		X				X
Maine									X
Massachusetts								X	X
Michigan	X	X		X	X		X	X	X
Minnesota		X				X	X	X	
Mississippi					X				X
New Hampshire									X
New Jersey							X		X
New Mexico		X			X				X
New York		X	X					X	X
North Carolina	X	X	X	X	X	X	X	X	X
Ohio		X							
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon		X						X	X
Puerto Rico	X	X	X	X	X	X	X		X
Rhode Island									X
Utah									X
Vermont	X	X		X		X			X
Washington		X	X	X		X			X
West Virginia		X	X					X	X
Wisconsin	X	X	X	X	X				X
Wyoming							X		X
Total	11	22	10	11	12	11	14	11	30

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An empty cell indicates that no business practice was identified in association with that domain.

When state teams referred to the legal requirements surrounding this scenario's activities, to determine whether the researcher could "piggyback" his work onto the existing protocol without further IRB review, the Legal Working Group (LWG) stakeholders discussed the relevance of specific Code of Federal Regulations citations that address patient "waivers of authorization." LWG members also referred to the need to review the requested research protocol to discern whether it followed Code of Federal Regulations provisions that require new IRB approval when the original IRB approval period lapses. Although state teams made reference to their own state laws for other scenarios in their reports, a majority of the state teams thought that the federal HIPAA statutes would guide their decisions in this scenario's topic area.

Although state teams agreed that the IRB patient protections were the central topic, they reported that their stakeholders differed over whether these protections limited data sharing or whether they were simply neutral with respect to data sharing. State teams generally reported that their stakeholders recognized the importance of protecting patients against illegitimate or unethical uses of their data, although some stakeholders did perceive IRB requirements as burdensome, arguing that IRBs unnecessarily delay or limit the scope of important research.

State teams uniformly discussed the confusion surrounding IRB requirements for research protocols and, though not directly relevant to this scenario, the special opportunities for confusion when there are multiple research sites and multiple IRBs. Often it is not clear to institutions or researchers what limitations IRBs impose on data release.

2.5 Law Enforcement (Scenario 8)

8. Scenario for Access by Law Enforcement

An injured 19-year-old college student is brought to the ER following an automobile accident. It is standard to run blood-alcohol and drug screens. The police officer investigating the accident arrives in the ER, claiming that the patient may have caused the accident. The patient's parents arrive shortly afterward. The police officer requests a copy of the blood-alcohol test results, and the parents want to review the ER record and lab results to see if their child tested positive for drugs. These requests to print directly from the electronic health record are made to the ER staff.

The patient is covered under his parent's health and auto insurance policy.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. County contracts with emergency department to perform blood-alcohol test draws.
2. Printing of additional copies of medical record reports for parents, insurance companies, and police.
3. Asking patient if it is okay to talk to parents or give information to parents about their condition.
4. Communication with primary care provider.

2.5.1 Stakeholders

Overall, the state teams were able to include a wide variety of stakeholders in discussions for Scenario 8. The average number of stakeholder groups with input to the scenario was 3.3. Three states, however, were able to draw from more than 7 different stakeholder groups. Although this scenario had a significant law enforcement component, less than 50% of the state teams were able to secure the participation of law enforcement personnel in the discussion. This potential bias was noted by the state teams themselves, and the majority of the teams noted that lack of input from law enforcement personnel was a significant issue that they would be working to address before drafting the final Variations Working Group (VWG) report.

Although the stakeholder variation among state teams was great, 26 of the 34 states included a hospital physician stakeholder in discussions, and 16 of the 34 included clinicians or physicians. These stakeholders, along with consumers who were engaged by 10 of the 34 state teams, are the groups that would be most directly affected by this scenario (Table 2-9).

Table 2-9. Stakeholder Groups Engaged in Scenario 8 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenario 8 (N = 34)
Hospitals	26 (76%)
Physician groups	16 (47%)
Law enforcement	13 (38%)
Clinicians	11 (32%)
Consumers/consumer organizations	10 (29%)
State government	7 (20%)
Payers/insurance	6 (18%
Public health agencies	6 (18%)
Laboratories	4 (12%)
Community clinics	4 (12%)
Federal health facilities	3 (9%)
Emergency services	2 (6%)
Long-term care facilities/nursing homes	2 (6%)
Homecare and hospice	1 (3%)
Pharmacies	1 (3%)
Professional associations	1 (3%)

2.5.2 Domains

Wide variation emerged in how the state teams viewed this scenario. Some states felt that all 9 domains were relevant to this scenario, while other states felt that this scenario involved only 1 or 2 domains (Table 2-10).

Despite this variation among the state teams, 30 of the 34 teams stated that Domain 9—"Information use and disclosure policies that arise as health care entities share clinical information electronically"—was valid for this scenario. Most state teams agreed that hospitals must receive formal service of a subpoena before information can be released to law enforcement. However, several state teams noted that they were aware of variations in responses to law enforcement requests among emergency departments in their states, with some departments being more willing than others to release information on the basis of a verbal request rather than a formal subpoena. State teams generally agreed that variations in business practices occur because health care organizations and law enforcement do not seem entirely sure about the law and because interpretation of HIPAA varies. A related concern expressed by at least 5 states addressed the issue of the inadequacy of confidentiality training.

All the state teams were in agreement that no information would be released to the parents of an adult child. A small group of state teams (5), however, included some discussion of the fact that hospitals handle the presence of parents of adult children patients in the emergency department in nonstandard and varying ways.

2.5.3 Critical Observations

A common theme among the state teams was that this scenario reveals a clear chasm between the medical community and law enforcement, and this chasm severely restricts the exchange of information. Because law enforcement personnel reported that they try to obtain as much information as possible before transporting a person to a hospital, several state teams noted how each group's lack of understanding and their differing roles could impact the treatment of the person detained. Law enforcement considered the delay in transportation a necessary operating procedure because difficulties in collecting information greatly increase once an injured person enters a medical facility.

Another critical observation related to the potential "run" around the privacy of the adult child's health information while he or she is covered by a parent's insurance. Several states noted that a parent's receipt of the explanation of benefits from the insurance agency would likely contain enough information about billing for the health care service to enable parents to learn medical information to which they would not otherwise be entitled. This situation could be viewed as a serious barrier to care if a person opted to forgo care because a related or unrelated third party was responsible for payment.

Table 2-10. Nine Privacy and Security Domains Affected by Business Practices Associated With Scenario 8 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X		X	X				
Arizona									X
Arkansas		X		X	X			X	X
California									X
Colorado									X
Connecticut	X	X	X	X	X	X	X	X	X
Florida		X				X		X	
Illinois		X							
Indiana								X	X
Iowa		X						X	X
Kansas		X	X	X		X			X
Kentucky		X						X	X
Louisiana		X					X	X	X
Maine								X	X
Massachusetts									X
Michigan	X	X		X		X	X		X
Minnesota	X	X				X	X	X	X
Mississippi									X
New Hampshire									X
New Jersey	X							X	X
New Mexico									X
New York		X		X		X	X		X
North Carolina	X	X	X	X	X	X	X	X	X
Ohio								X	X
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon		X						X	X
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island									X
Utah									X
Vermont	X	X		X		X		X	
Washington									X
West Virginia	X	X	X	X	X	X	X	X	X
Wisconsin	X	X	X	X		X		X	X
Wyoming									X
Total	11	19	7	12	7	12	9	18	30

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An empty cell indicates that no business practice was identified in association with that domain.

2.6 Prescription Drug Use (Scenarios 9 and 10)

9. Pharmacy Benefit Scenario A

The Pharmacy Benefit Manager (PBM) has a mail order pharmacy for a hospital that is self-insured and also has a closed formulary. The PBM receives a prescription from Patient X, an employee of the hospital, for the antipsychotic medication Geodon. The PBM's preferred alternatives for antipsychotics are Risperidone (Risperdal), Quetiapine (Seroquel), and Aripiprazole (Abilify). Since Geodon is not on the preferred alternatives list, the PBM sends a request to the prescribing physician to complete a prior authorization in order to fill and pay for the Geodon prescription. The PBM is in a different state than the provider's outpatient clinic.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Patient authorization to share information with the PBM.
2. Agreements for data sharing—business associate agreements.
3. Health care provider must determine minimum necessary access to PHI.
4. If allowed, role and access management are issues.
5. Determine method for enabling secure remote access if allowed.

10. Pharmacy Benefit Scenario B

A PBM (PBM1) has an agreement with Company A to review the companies' employees' prescription drug use and the associated costs of the drugs prescribed. The objective would be to see if PBM1 could save the company money on their prescription drug benefit. Company A is self-insured and, as part of their current benefits package, they have the prescription drug claims submitted through their current PBM (PBM2). PBM1 has requested that Company A send their electronic claims to them to complete the review.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Business associate agreements and formal contracts exist between Company A and the PBMs.
2. The extent and amount of information shared between the various parties would be limited by the minimum necessary guidelines.

2.6.1 Stakeholders

For Scenario 9, RTI suggested that community clinics and health centers, pharmacies, and consumers (patients) should be engaged in the review of the scenario and asked to describe business practices. Additional stakeholder groups that might be able to describe practices associated with the scenario included clinicians, physician groups, and payers.

For Scenario 10, RTI suggested that, at a minimum, pharmacies, consumers (employees), and employers should be engaged in the review, and that clinicians, physician groups, payers, and community clinics and health centers might be able to provide additional insight.

All stakeholder groups except law enforcement were engaged in the review of Scenarios 9 and 10 by at least one project team (Table 2-11).

Table 2-11. Stakeholder Groups Engaged in Scenario 9 and 10 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenarios 9 and 10 (N = 34)
Pharmacies/PBMs	25 (73%)
Payers	18 (53%)
Physician groups	16 (47%)
Clinicians	15 (44%)
Hospital personnel/emergency room staff	15 (44%)
Consumers (patients/employees)	12 (35%)
Employers	11 (32%)
Community clinics and health centers	10 (29%)
State government	8 (24%)
Other	6 (18%)
Federal health facilities	5 (15%)
Professional associations	5 (15%)
Researchers	4 (12%)
Public health agencies	3 (9%)
Long-term care facilities/nursing homes	3 (9%)
Homecare and hospice	3 (9%)
Laboratories	1 (3%)
Quality improvement organizations	1 (3%)

The relevant stakeholder groups identified by RTI were the most frequently engaged stakeholder groups. The only addition among the 8 most frequently engaged groups was hospitals. Nine project teams did not report engaging pharmacies or PBMs. Three of the 6 "other" stakeholders were associated with mental health care and were asked to review Scenario 10.

2.6.2 Domains

Wide variation across states emerged, with 6 state teams reporting that 8 or 9 domains of privacy and security were affected by business practices, and 10 state teams reporting that only 1 or 2 domains were affected. The 3 most frequently cited domains were 9—"Information use and disclosure policies" (27 states), 4—"Transmission security" (24 states), and 2—"Authorization and access control" (19 states; Table 2-12).

Table 2-12. Nine Privacy and Security Domains Affected by Business Practices Associated With Scenarios 9 and 10 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X	X	X			X		
Arizona	X	X	X	X		X	X		
Arkansas	X	X	X	X		X	X	X	X
California									X
Colorado				X					X
Connecticut	X	X	X	X	X	X	X	X	X
Florida				X					X
Illinois	X			X			X		X
Indiana			X	X				X	X
Iowa		X		X			X		X
Kansas	X	X	X	X	X	X	X		X
Kentucky	X	X		X	X	X	X	X	X
Louisiana									
Maine				X				X	X
Massachusetts		X		X					X
Michigan		X		X					X
Minnesota								X	
Mississippi		X		X					X
New Hampshire			X	X					
New Jersey		X		X					
New Mexico	X	X	X	X	X		X	X	X
New York		X				X			X
North Carolina	X	X	X	X	X	X	X	X	X
Ohio	X								X
Oklahoma	X	X	X	X		X			X
Oregon							X	X	X
Puerto Rico	X			X			X		X
Rhode Island									X
Utah							X		
Vermont		X		X					X
Washington	X			X			X	X	X
West Virginia	X	X					X	X	X
Wisconsin	X	X	X	X		X		X	X
Wyoming		X							X
Total	15 (44%)	19 (56%)	11 (32%)	24 (71%)	5 (15%)	9 (26%)	15 (44%)	12 (35%)	27 (79%

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An empty cell indicates that no business practice was identified in association with that domain.

BAAs and *minimum necessary* were the most common issues raised in discussions of Domain 9—"Information use and disclosure policies." Many state teams noted that a BAA had to exist for the exchange of information to be allowed. There was general agreement that HIPAA would protect identifiable patient information if this business relationship existed. Many state teams noted that the patient would be informed of this relationship and the potential need for information sharing at the time of enrollment. Regarding *minimum necessary,* many states noted that the provider is responsible for ensuring that the *minimum necessary* information is disclosed.

Many state teams reported that most of the information described in these scenarios is being exchanged by fax or telephone and that practices are in place to ensure that these exchanges are secure. These state teams expressly noted avoidance of e-mail exchange or use of advanced technology to exchange data in these scenarios. Other states have begun to exchange pharmacy data via virtual private network (VPN). They also have some experience with e-prescribing, which introduces complexity because of the need to comply with the special federal regulations governing controlled substances.

Discussions of Domain 2 addressed the BAA as described under Domain 9. States reported that these agreements provided both parties security practice knowledge sufficient to enable the information exchange.

2.6.3 Critical Observations

Critical observations concerning Scenarios 9 and 10 are as follows:

- Exchange of pharmacy data is largely paper based at present, relying heavily on fax and telephone.
- Many state teams reported that lack of trust in security between organizations is a major barrier to interoperable eHIE.
- Pharmacy data are particularly subject to requests from marketing. Stakeholders currently invoke HIPAA to limit release of pharmacy data.
- States have requested clarification of the relationship between the federal Employee Retirement Income Security Act and state requirements.

2.7 Health Care Operations/Marketing (Scenarios 11 and 12)

11. Healthcare Operations and Marketing Scenario A

ABC Health Care is an integrated health delivery system composed of 10 critical access hospitals and one large tertiary hospital, DEF Medical Center, which has served as the system's primary referral center. Recently, DEF Medical Center has expanded its rehab services and created a state-of-the-art, stand-alone rehab center. Six months into operation, ABC Health Care does not feel that the rehab center is being fully utilized and is questioning the lack of rehab referrals from the critical access hospitals.

ABC Health Care has requested that its critical access hospitals submit monthly reports containing patient-identifiable data to the system six-sigma team to analyze patient

encounters and trends for the following rehab diagnoses/procedures:

- Cerebrovascular accident (CVA)
- Hip fracture
- Total joint replacement

Additionally, ABC Health Care is requesting that this same information, along with individual patient demographic information, be provided to the system Marketing Department. The Marketing Department plans to distribute to these individuals a brochure highlighting the new rehab center and the enhanced services available.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Decision to conduct marketing using PHI with their consumers.
2. Authorization from consumer to allow IHDS to market to themselves.
3. Determine mode of transferring information and type of information, ie, identifiable or de-identified information to the marketing department.

12. Healthcare Operations and Marketing Scenario B

ABC hospital has approximately 3,600 births per year. The hospital marketing department is requesting identifiable data on all deliveries, including mother's demographic information and birth outcome (to ensure that contact is made only with those deliveries resulting in healthy live births).

The marketing department has explained that they will use the patient information for the following purposes:

1. To provide information on the hospital's new pediatric wing/services.
2. To solicit registration for the hospital's parenting classes.
3. To request donations for construction of the proposed neonatal intensive care unit.
4. To sell the data to a local diaper company to use in marketing diaper services directly to parents.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Requesting patient consent or permission to use and sell identifiable data for marketing purposes.
2. Decisions to conduct marketing using patient data.
3. Determining mode of transferring information and type of information, ie, identifiable or de-identified information to the marketing department.

2.7.1 Stakeholders

Scenario 11 engaged stakeholders from hospitals, community clinics, and health centers. The scenario could easily be modified to apply to any provider wishing to market services to a targeted subset of patients. Thus, other relevant stakeholder groups included clinicians, physician groups, federal health facilities, payers, laboratories, pharmacies, long-term care facilities and nursing homes, homecare and hospice, and consumers.

Scenario 12 engaged stakeholders from hospitals, as well as consumers and employers. Also recommended were clinicians, physician groups, federal health facilities, payers, community clinics and health centers, laboratories, pharmacies, long-term care facilities, nursing homes, homecare and hospice, and law enforcement.

All stakeholder groups except law enforcement were engaged in the review of Scenarios 11 and 12 (Table 2-13). The most frequently engaged stakeholder group was hospitals, engaged by 29 of the 34 state project teams. Clinicians, community clinics, consumers, physician groups, and payers were a distant second tier of stakeholder groups, each being engaged in discussions for 8 to 10 states.

Table 2-13. Stakeholder Groups Engaged in Scenario 11 and 12 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenarios 11 and 12
Hospital personnel/emergency room staff	29 (85%)
Clinicians	10 (29%)
Community clinics and health centers	9 (26%)
Consumers (patients)	9 (26%)
Physician groups	8 (24%)
Payers	8 (24%)
Professional associations	6 (18%)
Federal health facilities	6 (18%
Homecare and hospice	5 (15%)
Researchers	5 (15%)
State government	5 (15%)
Public health agencies	4 (12%)
Pharmacies	4 (12%)
Long-term care facilities/nursing homes	4 (12%)
Laboratories	2 (6%)
Employers	2 (6%)
Quality improvement organizations	1 (3%)

2.7.2 Domains

Wide variation among state teams emerged regarding domains, with 3 state teams reporting that 8 or 9 domains of privacy and security were affected, while 18 state teams reported that only 1 or 2 domains were affected. By far the most frequently cited domain was Domain 9—"Information use and disclosure policies" (32 states), followed distantly by Domain 2—"Authorization and access control" (18 states; Table 2-14).

Most state teams reported that organizations felt they had clear policies governing what activities were defined as marketing and what information could be shared for marketing purposes. Sharing patient data for Six Sigma quality improvement was widely seen as health care operations, not marketing, and therefore permissible under HIPAA. Most state teams reported that using aggregated data for this purpose was allowed. Also, most state teams were certain that using patient-identified information for marketing purposes was not

Table 2-14. Nine Privacy and Security Domains Affected by Business Practices Associated With Scenarios 11 and 12 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska		X				X	X	X	X
Arizona			X	X	X		X		
Arkansas		X		X			X		X
California						X			X
Colorado									X
Connecticut	X	X	X	X	X	X	X		X
Florida		X							X
Illinois				X					X
Indiana		X				X			X
Iowa		X							X
Kansas	X	X	X			X		X	X
Kentucky									X
Louisiana		X	X			X	X		X
Maine							X	X	X
Massachusetts									X
Michigan									X
Minnesota		X				X			X
Mississippi				X					X
New Hampshire									X
New Jersey		X							X
New Mexico		X	X				X	X	X
New York	X	X		X		X	X		X
North Carolina	X	X	X	X	X	X	X	X	X
Ohio		X							X
Oklahoma	X	X	X	X	X	X	X		X
Oregon	X	X		X			X		
Puerto Rico								X	X
Rhode Island									X
Utah								X	X
Vermont									X
Washington		X				X	X		X
West Virginia									X
Wisconsin	X	X	X	X		X		X	X
Wyoming									X
Total	7 (21%)	18 (53%)	8 (24%)	10 (29%)	4 (12%)	12 (35%)	12 (35%)	8 (24%)	32 (94%)

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An empty cell indicates that no business practice was identified in association with that domain.

permitted without patient consent and would be unethical if permitted. Nearly all state teams agreed that they would never sell data for third-party marketing.

Many state teams reported that existing access controls prohibit access to the data for purposes of marketing. A few state teams reported that access would require the involvement of their IRB or privacy officer before access to data for marketing would be allowed.

2.7.3 Critical Observations

Responses to Scenario 11 were fairly uniform. This scenario described the internal use of patient data for quality improvement and marketing efforts that amount to the hospital's offering additional services to its existing customers. Most stakeholders felt the quality improvement use could be accomplished with de-identified data and did not present any areas where policy decisions might be needed.

State project teams reduced Scenario 12 to the different information exchanges described. Disclosure to sell patient data to a local diaper service was widely viewed as disallowed either by the individual states or by HIPAA. Most states viewed it as unethical behavior and would not sell such data even if allowed to by state law. Patient consent would be required before data could be sold. There was broad agreement that consumers would react negatively if their medical data were sold. This use would cause consumers to wonder who else had access to their medical data.

There was broad agreement that HIPAA allows hospitals to provide information on pediatric services and parenting classes and that HIPAA requires that patients have the opportunity to opt out of fundraising communications. Patient consent is required for marketing uses of identifiable patient data.

2.8 Public Health—Bioterrorism Event (Scenario 13)

13. Bioterrorism Event

A provider sees a person who has anthrax, as determined through lab tests. The lab submits a report on this case to the local public health department and notifies their organizational patient safety officer. The public health department in the adjacent county has been contacted and has confirmed that it is also seeing anthrax cases, and therefore this could be a possible bioterrorism event. Further investigation confirms that this is a bioterrorism event, and the state declares an emergency. This then shifts responsibility to a designated state authority to oversee and coordinate a response, and involves alerting law enforcement, hospitals, hazmat teams, and other partners, as well as informing the regional media to alert the public concerning symptoms and seeking treatment if feeling affected. The state also notifies the federal government of the event, and some federal agencies may have direct involvement in the event. All parties may need to be notified of specific identifiable demographic and medical details of each case as it arises to identify the source of the anthrax, locate and prosecute the parties responsible for distributing the anthrax, and protect the public from further infection.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Providing patient-specific information related to specific symptoms to law enforcement, CDC, Homeland Security, and health department in a situation where a threat is being investigated.

2.8.1 Stakeholders

Scenario 13 was reported by many state teams as one of the more popular scenarios for discussion. Overall, the state teams were able to include a wide variety of stakeholders in discussions for Scenario 13 (Table 2-15). The average number of stakeholder groups offering input to the scenario discussion was 4. However, 12 states were able to secure input from 5 or more stakeholder groups, and 2 states were able to draw from more than 10 different stakeholder groups. Given the significant public health component of this scenario, stakeholders from this sector were successfully brought into the discussion by all but a few states. Those states that did not have direct input from public health were able to bring information from state agency and federal agency staff familiar with public health procedures. This scenario, like Scenario 8, had a significant law enforcement component, and, again, lack of participation by stakeholders from the community was noticeable, with fewer than 10 states reporting input from it.

Between 15 and 20 states included a hospital physician stakeholder in discussions, and 13 of the 34 included either state or federal agency stakeholder input. Given the media relations component of the scenario and the threat to the public, it was somewhat surprising that only about one third of the states were able to include consumer stakeholders in their discussions.

2.8.2 Domains

Wide variation emerged in how the state teams viewed this scenario (Table 2-16). Five state teams felt that all 9 domains were relevant to this scenario, while 7 other state teams felt that this scenario involved only 1 to 3 domains. The majority of states' business practices fell within 4 to 7 domains.

Despite this variation among the states, 17 of the 34 state teams said that Domains 2—"Information authorization and access controls," 4—"Information transmission security or exchange protocols," and 8—"State law restrictions" were the more closely related to this scenario. Most state teams were in general (but not complete) agreement that required disease reporting superseded all patient confidentiality. States were aware that HIPAA provides specific exemptions to accommodate this requirement. Furthermore, many states suggested that in addition, for notification purposes, the good of the community would make the privacy and security of health information secondary to treatment during the event. Several state teams reported widespread misunderstanding about what state law requires for verification or authorization of the data and for tracking automated release

Table 2-15. Stakeholder Groups Engaged in Scenario 13 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenario 13 (N = 34)
Public health agencies	27 (79%)
Physician groups	16 (47%)
Clinicians	16 (47%)
Hospital personnel/emergency room staff	15 (44%)
State government	13 (38%)
Laboratories	11 (32%)
Consumers	10 (29%)
Federal health facilities	8 (26%)
Emergency services	5 (15%
Law enforcement	5 (15%)
Homecare and hospice	5 (15%)
Payers/insurance	4 (12%)
Community clinics and health centers	4 (12%)
Pharmacies	3 (9%)
Mental health	2 (6%)
Emergency services	2 (6%)
Long-term care facilities/nursing homes	2 (6%)
Medical and public health schools that undertake research	2 (6%)
Professional associations	2 (6%)
Poison control	1 (3%)

of data in such a scenario. At least 6 state teams noted that many providers and clinicians in their states do not understand the state law and regulatory reporting requirements during suspected bioterrorism or during a potential epidemic and that this misunderstanding results in broad variation in practice. It was often noted that this scenario presented very clear differences in practices, depending on whether the organizations were using a paper-based or an electronic system.

2.8.3 Critical Observations

A common theme found in the state team reports is that state law and regulations are not yet sufficient to ensure private and secure electronic exchange of health data with mandating stakeholders, such as law enforcement. A particularly critical observation noted by teams of states 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. Although it is not clear how these conflicting interests can

Table 2-16. Nine Privacy and Security Domains Affected by Business Practices Associated With Scenario 13 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X		X			X			
Arizona				X			X		X
Arkansas		X		X			X	X	
California					X	X			X
Colorado		X		X		X	X		X
Connecticut	X		X	X	X	X	X	X	X
Florida	X	X		X	X	X	X	X	X
Illinois	X	X			X				X
Indiana				X					X
Iowa		X							
Kansas	X	X	X	X	X		X	X	X
Kentucky									
Louisiana	X	X		X				X	X
Maine	X								X
Massachusetts									X
Michigan	X			X			X		X
Minnesota	X	X	X	X	X	X	X	X	X
Mississippi				X					
New Hampshire									x
New Jersey		X		X				X	
New Mexico									
New York	X	X	X				X	X	X
North Carolina		X						X	
Ohio								X	
Oklahoma	X	X	X	X	X	X	X	X	X
Oregon									
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island									X
Utah									
Vermont		X		X			X		X
Washington		X		X				X	X
West Virginia		X						X	X
Wisconsin	X	X	X	X	X	X	X	X	X
Wyoming								X	X
Total	13	17	8	17	9	9	13	16	22

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An empty cell indicates that no business practice was identified in association with that domain.

best be reconciled, it is critical that this issue be addressed, because the ability to find relatives admitted to hospitals during an emergency is an important area of public concern.

2.9 Employee Health Information Scenario (Scenario 14)

14. Employee Health Information Scenario

An employee (of any company) presents in the local emergency department for treatment of a chronic condition that has worsened but is not work related. The employee's condition necessitates a 4-day leave from work for illness. The employer requires a "return to work" document for any illness requiring more than 2 days' leave. The hospital Emergency Department has an EHR, and their practice is to cut and paste patient information directly from the EHR and transmit the information via e-mail to the Human Resources department of the patient's employer.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Determining employee agreement to release information.
2. Determining what are the minimum necessary elements that can legally be transmitted.
3. Ensuring the data are secured as they are transmitted.

2.9.1 Stakeholders

The state teams identified the appropriate stakeholders to review Scenario 14 and to discuss how their current business practices address the scenario in relationship to the 9 domains of interoperability. The range of stakeholders was generally broad, as were the various roles of the discussants (see Appendix A for a complete list of stakeholders). Their current business practices provided the opportunity for the states to examine the current system and to explore ways to improve or enhance the business practice. Table 2-17 shows the distribution of stakeholders reviewing Scenario 14.

The hospital stakeholders that have yet to transition to an electronic system and that continue to use hard-copy forms reported that their policy was to release a form that identified only the days the patient was off or the days the patient was to return to work. Stakeholders agreed that no PHI would be released by paper or electronically without a signed release of information from the patient. All interviewed stakeholders stated that a patient must initiate the request for return-to-work documentation; employers are not permitted to request the information directly.

Hospitals and physicians are careful to release only the *minimum necessary* information to satisfy employers' requests and will not reveal diagnosis-related PHI. Employers are aware of—and wary of—the liability associated with knowledge of their employees' health information. Consequently, many employers do not request diagnosis-related PHI. Hospitals and physicians respect that a patient authorization to release information to an employer is limited to the current request and does not extend to future requests. In general, the stakeholders were diligent in distinguishing between an inhibitor to electronic information exchange and measures of security; that is, stakeholders appreciate the value

Table 2-17. Stakeholder Groups Engaged in Scenario 14 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder in Review of Scenario 14 (N = 34)
Hospital personnel/emergency room staff	26 (76%)
Consumers/consumer organizations	14 (41%)
Employers	10 (29%)
Clinicians	9 (26%)
Physician groups	7 (21%)
Payers	5 (15%)
Community clinics and health centers	5 (15%)
Federal health facilities	5 (15%)
Public health agencies	5 (15%)
State agencies	4 (12%)
Legal/compliance community	4 (12%)
Other	4 (12%)
Homecare and hospice	2 (6%)
Professional associations	2 (6%)
Researchers	2 (6%)
Law enforcement/corrections	2 (6%)
IT	2 (6%)
Long-term care facilities/nursing homes	1 (3%)
Mental health agencies	1 (3%)
Laboratories	1 (3%)
Pharmacies/PBMs	1 (3%)

of interoperability, but they are reluctant to forgo safeguards of consumer confidentiality for the sake of easy data exchange.

Discussion ensued about the use of e-mail and other electronic forms of transmission. Most stakeholders agreed that e-mail is not secure without encryption. Other stakeholders agreed that when a provider cuts and pastes information from an EHR he or she must be careful not to include any PHI without obtaining the patient's signed consent. Discussants reported that PHI is not usually transmitted to an employer via e-mail. Most often a letter summarizing treatment or a doctor's note is presented in person by the employee or is faxed with an appropriate cover sheet by the treating facility.

When PHI is transmitted electronically, the HIPAA security regulations govern that transmission. Among other things, such standards require covered entities to implement procedures to verify the identity of a person or entity seeking access to electronic PHI and to implement security measures to guard against unauthorized access to electronic PHI.

Furthermore, covered entities are required to implement measures to protect electronic PHI from unauthorized access during transmission.

Other physical safeguards used to protect employee health information include filing patient health information separately from personnel files and locking employee medical records behind double-locked doors in a separate room within the Human Resources (HR) department. Health care institutions reported that they require their employees to undergo training on confidentiality policies, and their employees are required to sign an agreement that PHI is accessed and viewed only for treatment, payment, or operational purposes pertaining to job duties.

Practices and policies associated with administrative safeguards are required to protect electronic PHI and to manage the conduct of the covered entity's workforce. Covered entities must limit physical access while permitting properly authorized access. The specific standards cover facility access controls, workstation use, workstation security, and device and media controls.

2.9.2 Domains

Although all the domains were identified as relevant to the scenario (Table 2-18), the following domains were cited more often than the others by the stakeholders:

- Domain 9—"Information use and disclosure policies that arise as health care entities share clinical health information electronically,"
- Domain 4—"Information transmission security or exchange protocols (ie, encryption) for information that is being exchanged over an electronic communications network,"
- Domain 2—"Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information," and
- Domain 1—"User and entity authentication to verify that a person or entity seeking access to electronic personal health information is who they claim to be."

2.9.3 Critical Observations

Some stakeholders considered this scenario to be among the least problematic of the scenarios they were to analyze. They felt that, regardless of size, most health care organizations are keenly aware of the return-to-work rules in their state, because they provide the documentation for the return-to-work forms. In larger organizations, there is an occupational health manager in the HR department who will instruct the employee's manager on the nature of work restrictions and their duration. There are no identified cases in which an individual was asked for PHI.

The VWG determined that emergency rooms will not transmit PHI to any nonmedical organization unless that institution has a BAA with the requester, and employers do not expect to receive information from the emergency room electronically. Generally, an

Table 2-18. Nine Privacy and Security Domains Affected by Business Practices Associated With Scenario 14 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X	X						
Arizona		X	X	X				X	
Arkansas	X		X			X	X		X
California		X		X					X
Colorado				X			X		X
Connecticut	X	X	X						
Florida		X		X					X
Illinois	X	X		X	X				X
Indiana				X	X				X
Iowa									X
Kansas			X						X
Kentucky				X					X
Louisiana			X	X	X	X		X	X
Maine				X					X
Massachusetts				X				X	X
Michigan	X			X			X		X
Minnesota		X		X	X	X		X	
Mississippi				X					X
New Hampshire	X	X		X	X			X	X
New Jersey		X		X			X		
New Mexico	X	X		X					X
New York		X		X					X
North Carolina	X	X	X	X	X	X	X	X	X
Ohio		X							
Oklahoma	X	X		X			X	X	X
Oregon				X			X		X
Puerto Rico	X	X	X	X	X	X	X		
Rhode Island									X
Utah		X							X
Vermont			X				X		X
Washington		X							X
West Virginia	X	X	X	X		X	X	X	X
Wisconsin				X		X		X	X
Wyoming			X						X
Total	11	18	11	23	7	7	10	9	27

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An empty cell indicates that no business practice was identified in association with that domain.

employer's terms of employment or organizational policy require that specific information about the employee's health problem be shared in only a couple of instances: (1) if the length of time the employee would be absent from work triggers a claim for temporary disability or workers' compensation, or (2) if the employee is performing direct care and needs to be certified as free of any communicable disease. Transmission of the prescription form or letter from a doctor is usually by hand, mail, or fax. Employers reported that they stored medical information separately from their other employee records—in a locked filing cabinet in a secure location accessible only to specifically assigned and authorized staff.

Nevertheless, one state team identified highly variable business practices with respect to the disclosure of individualized health information by health care providers to employers. Because of the relative ease in retrieving larger amounts of information from an EHR system and the ability to quickly and cheaply transmit such information, the implementation of an interoperable EHR system will make this issue an even tougher one for all concerned. The stakeholders for this state acknowledged the need to reach greater consensus on the appropriate checks and balances to be used in communicating such information to employers without sacrificing any more patient privacy than is necessary.

The main business practice raised by this scenario concerned procedures for communicating with a patient's employer about the patient's ability to return to work. Organizations interpreted privacy responsibility issues variably as applied to such communication with the patient's employer. Some stakeholders removed themselves from the situation by releasing information only directly to the patient. The patient was then responsible for delivering the return-to-work form to the employer. Others said they would provide a note directly to the employer upon the patient's request. All stakeholders agreed that no treatment or diagnosis information was required in return-to-work documentation.

Hospital stakeholders with an EHR stated that they would not cut and paste any information from the EHR; however, some EHRs have a software-generated letter on the hospital's letterhead that contains the *minimum necessary* information, which includes treatment dates, return-to-work date, and any physical limitations. Stakeholders without an EHR stated that they use standard forms with hospital logo that contain the *minimum necessary* information: treatment dates, return-to-work dates, and any physical limitations.

Consumers were most concerned about the following groups accessing their PHI: employers, insurance companies, the government, schools, and marketing entities. Regarding employers, the concerns were that the information would be used against employees in hiring decisions, reduction in force, promotion decisions, and the like. Also, employees do not want employers to know about sensitive mental health conditions like depression or substance abuse problems, or even about chronic illnesses or medical problems requiring expensive drugs or frequent service use.

2.10 Public Health (Scenarios 15–17)

15. Public Health Scenario A—Active Carrier, Communicable Disease Notification

A patient with active TB, still under treatment, has decided to move to a desert community that focuses on spiritual healing, without informing his physician. The TB is classified MDR (multidrug resistant). The patient purchases a bus ticket—the bus ride will take a total of 9 hours with 2 rest stops across several states. State A is made aware of the patient's intent 2 hours after the bus with the patient leaves. State A now needs to contact the bus company and other states with the relevant information.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Providing patient-specific information related to a specific communicable disease to law enforcement, non–health-care entities, and health department in a situation where a threat is being responded to.
2. Ensuring the data are secured as they are transmitted.

16. Public Health Scenario B—Newborn Screening

A newborn's screening test comes up positive for a state-mandated screening test, and the state lab test results are made available to the child's physicians and specialty care centers specializing in the disorder via an Interactive Voice Response (IVR) system. The state lab also enters the information in its registry and tracks the child over time through the child's physicians. The state public health department provides services for this disorder and notifies the physician that the child is eligible for those programs.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Providing patient-specific information related to specific symptoms of a disease to a health department in a situation where a targeted disease is being investigated.

17. Public Health Scenario C—Homeless Shelters

A homeless man arrives at a county shelter and is found to be a drug addict and in need of medical care. This person does have a primary care provider, and he is sent there for medical care. Primary care provider refers patient to a hospital-affiliated drug treatment clinic for his addiction under a county program. The addiction center must report treatment information back to the county for program reimbursement and back to the shelter to verify that the person is in treatment. Someone claiming to be a relation of the homeless man requests information from the homeless shelter on all the health services the man has received. The staff at the homeless shelter are working to connect the homeless man with his relative.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. The extent and amount of information shared between the various facilities would be limited by the minimum necessary guidelines.

2.10.1 Stakeholders

Although a wide variety of stakeholders contributed to these scenarios across the 34 participating states, most input for Scenarios 15 and 16 came from public health agencies, with almost all state teams mentioning input from a public health agency representative (94%) specifically when discussing these scenarios (Table 2-19). In many cases, additional input was gathered from laboratories and clinicians. For most states, Scenario 17 generated more widespread input than Scenarios 15 and 16: although public health and state government agencies were still strongly represented, there was also strong representation from hospitals, state government, and physician groups. There were also notable contributions from homeless shelters in some states.

Table 2-19. Stakeholder Groups Engaged in Scenario 15–17 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenarios 15–17 (N = 34)
Public health agencies	32 (94%)
Hospital personnel/emergency room staff	16 (47%)
State government	14 (41%)
Physician groups	14 (41%)
Clinicians	13 (38%)
Laboratories	13 (38%)
Community clinics and health centers	11 (32%)
Correctional facilities/law enforcement	8 (24%)
Consumers/consumer organizations	8 (24%)
Federal health facilities	7 (21%)
Medical and public health schools that undertake research	6 (18%)
Payers	5 (15%)
Professional associations	4 (12%)
Homecare and hospice	4 (12%)
Long-term care facilities/nursing homes	3 (9%)
Pharmacies	3 (9%)
Homeless shelters	3 (9%)
Privacy officers	1 (3%)
Health care attorneys	1 (3%)
RHIOs	1 (3%)

2.10.2 Domains

The business practices collected for this scenario group focused on information exchange in public health, state government, and health oversight situations. As in other scenario

groups, some state teams discussed how these scenarios touched on all 9 domains; however, there were clearly some domains cited more frequently than others (Table 2-20).

Domain 9 (27 out of 34 states): Information Use and Disclosure Policy

Domain 9—"Information use and disclosure policy" was referenced most often, with 27 out of 34 state teams explicitly including discussions about business practices related to this domain. Although this domain clearly is important in discussions of public health issues, the actual business practices regarding use and disclosure in these scenarios are relatively consistent when compared to other scenario groupings.

This consistency is especially true in Scenario 15. All state teams agreed that the provider's disclosure of the patient's condition is permitted pursuant to section 164.512 of HIPAA regulations in the case of tuberculosis (TB). In most states, the primary contact occurs between public health entities using interjurisdictional notification from one state to another. Once communication has been established, there is no noted resistance to the idea of exchanging the patient's personal health information. The one clear exception exists in Puerto Rico, where there currently is no agreement between public entities to communicate anything other than demographic data.

Some variation emerged among state teams as to how much information was to be disclosed to either law enforcement or the bus company. Most state teams said that their public health agencies would share communicable-disease information with law enforcement and other entities (eg, transportation companies), but the level of information shared differed. For example, some states would allow the public health departments to notify the transportation company of the incident but would not disclose the identity of the patient, whereas other states would identify the patient to the transportation company but would not disclose the diagnosis. One exception to this general rule is Utah, where there are no rules governing the disclosure of information to either law enforcement or other entities; therefore, they generally *do not* disclose information. This nondisclosure often creates a conflict with law enforcement personnel, who feel it impedes their ability to do their jobs.

In terms of release of information to passengers, few state teams mentioned the idea of releasing PHI of the infected individual to passengers, because doing so was not necessary to contain the threat to public health. However, most state teams discussed disclosure of exposure in general to the passengers. Some states will notify passengers directly of their exposure, allowing the local public health office at the site of interception to manage the initial disclosure. Most also relied upon contact with the exposed individual's local public health department to follow up with the bulk of responsibilities, including release of follow-up information concerning their exposure and testing.

With Scenario 16 there was also minor variation among states. All state teams recognized the right to collect and store data in a disease registry for public health reporting purposes;

Table 2-20. Nine Privacy and Security Domains Affected by Business Practices Associated With Scenarios 15–17 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska	X	X				X	X		
Arizona				X				X	X
Arkansas			X	X				X	X
California						X	X	X	X
Colorado				X				X	X
Connecticut	X	X	X	X	X	X	X	X	X
Florida		X						X	X
Illinois	X	X		X		X	X		X
Indiana[a]		X	X	X					
Iowa[a]		X	X	X	X		X	X	X
Kansas	X	X	X	X	X	X	X	X	X
Kentucky	X			X				X	X
Louisiana	X	X	X	X			X	X	X
Maine[a]								X	X
Massachusetts	X							X	X
Michigan	X	X	X	X	X		X	X	X
Minnesota	X	X	X	X	X	X	X	X	X
Mississippi				X			X		X
New Hampshire		X							X
New Jersey[a]		X	X	X				X	X
New Mexico	X	X	X			X		X	
New York[b]	X	X	X				X		X
North Carolina[b]	X	X	X	X	X	X	X	X	X
Ohio[a]		X		X				X	
Oklahoma	X	X							X
Oregon		X		X			X	X	X
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island									
Utah								X	
Vermont	X			X	X				X
Washington	X		X	X			X	X	X
West Virginia		X	X	X				X	X
Wisconsin	X	X	X	X	X	X	X	X	X
Wyoming									X
Total	17 50%	21 62%	16 47%	22 65%	9 26%	11 32%	16 47%	23 68%	27 79%

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An empty cell indicates that no business practice was identified in association with that domain.

[a] State team combined Public Health Scenarios 15–17 with State Government Oversight Scenario 18.

[b] State team combined Public Health Scenarios 15–17 with Public Health-Bioterrorism Event Scenario 13.

however, variation exists in *how* and *to whom* the data are disclosed. Many of the states agreed that they would not disclose the information directly to a specialty care center, but instead would choose to disclose this information to the physician. In fact, a few state teams mentioned that the physician was the only source to whom they would release results of the tests. In almost all states, it is the providing physician's job to inform the parents about the services available for their child. In regard to disclosure to the parent, most states leave this disclosure up to the providing physician; however, in other states the public health department makes the disclosure directly to the parent by letter, which informs them directly about the specialty care service and centers that are available to them. There was no clear discussion of tracking additional treatment information for individual patients over time.

The variation in use and disclosure for Scenario 17 becomes broader. Most shelters providing input on the scenario agreed that disclosure of any health record information, even to a relative, would require written consent of the patient. However, a good number of state teams debated the shelter's covered entity status under HIPAA. Consequently, very few treatment programs reported that they would disclose information to the shelter. Although many state teams reported that homeless shelters would not, without written consent, even confirm or deny the presence of the patient to a relative, the fear of secondary disclosure in this exchange was extremely high.

The transmission of PHI, even for treatment purposes, between the primary care provider and drug treatment clinic requires written consent of the patient in most states. However, 32 states agree that the release of PHI for *payment* purposes is permissible without written consent under 45 C.F.R. § 164.506(a). Many stakeholders within the state referenced *minimum necessary* guidelines, although specifics concerning these guidelines were not clearly outlined in this section of the state reports, other than to say there were a multitude of interpretations across entities within the state. A few states cited the requirement of a business agreement between any entities claiming payment from a government program.

Domain 8 (23 out of 34 states): State Law Restrictions

All 3 scenarios within public health seemed to touch on business practices that mapped to Domain 8—"State law restrictions," and 23 of the state teams discussed this domain specifically. Many of the disclosure practices already discussed are governed by state law in order to outline practices that are permissible (but not mandated) under HIPAA. Although state law restrictions are mentioned in many of the state reports, they are not often deemed problematic to interoperability.

Regarding Scenario 15, most state teams specifically referenced the existence of laws mandating the reporting of TB, but laws governing the release of that information vary (see discussion of Domain 9) and often are misunderstood by stakeholders outside the public health entities.

There are a wider variety of laws governing the practices in Scenario 16. In most states, some type of newborn screening is mandatory. In states where the screening is not mandated by law, information is still routinely collected after consent is given as part of consent to treatment related to birth. Only 1 state reported an opt-out provision for the actual screening itself. This opt-out seemed to be tied to the state statute requiring additional provisions for the collection of genetic information.

More variable state law restrictions appear in terms of the release of the registry information (see previous Domain 9 discussion). Three states have an opt-out provision for their registry, which is usually presented as an option by the providing physician.

State teams were almost uniform in their discussion of the state law restrictions for Scenario 17, indicating that state laws impose greater restrictions on information exchange, even for treatment purposes, in substance abuse and mental health cases than in other cases. Although exchange of personal health information is often allowed for purposes of treatment or payment without written authorization by the patient, written authorization is almost always required for exchange of substance abuse or mental health information. This seems to be the practice, regardless of the existence of state law. Even in instances when exchange of information is permitted for treatment or billing, no team reported that its state would release this information to relatives without written consent of the patient.

Domain 4 (22 out of 34 states): Information Transmission Security or Exchange Protocols

For Scenario 15, transmission by telephone was the most common method because it was thought to be the most expedient and reliable form of data exchange in an emergency. Although some states have automated alert systems, these systems rarely cross state lines. The HIPAA Security Rule prohibits transmission of public health information by e-mail without encryption or similar protections. Currently, there is little or no discussion among states, even in geographic regions, about the security of their electronic systems, although this discussion might lead to eventual interstate data exchange between public health entities.

For Scenario 16, many state teams indicated that their state did not have an Interactive Voice Response (IVR) system comparable to the one presented in the scenario. Although the precise method of transmitting data varied among states, the majority of states collect information from a single state laboratory. In a minority of states, this process is not centralized; therefore, results are sent in from multiple laboratories. In states where multiple entities provide information for the registry, there is with each individual health care provider an agreement by which the registry uses and discloses information only as allowed by state statute. In all, the transmission between the laboratory and the registry in this scenario is likely to be electronic, especially if a central state laboratory is used. When electronic systems are not used, laboratories typically transmit information to the registry

by telephone or fax. States with more advanced EHR systems transmit laboratory data to the state public health agency by secure VPN. These electronic systems usually have a disclosure log to track all disclosures.

At least one state team also reported returning the lab results electronically to participating physicians by VPN, although this level of advancement is rare. Notification is often centralized from the registry, and physicians are usually notified only in the event of an abnormal or positive result. In most states, this communication is done by phone and in some cases by fax.

Scenario 17 involved a greater number of data exchanges than the others. However, there was broad consensus that, because there was very little electronic interoperability and because of the sensitive nature of the records being exchanged, most of these exchanges would occur by fax or mail if they were allowed to occur at all. Most providers did not report using e-mail, because there continues to be a lack of trust in it as a secure data transfer mode, especially when entities are discussing the transfer of mental health or substance abuse records.

Domain 2 (21 out of 34 states): Information Authorization and Access Controls

Within Domain 2, which covered information authorization and access controls, 21 state teams mentioned business practices. Most state teams agreed that exchange of information in an emergent situation or in the case of an imminent public health emergency does not require patient authorization. Exceptions do exist in the case of substance abuse and mental health records. The range of public health scenarios did unearth the differences in procedures when there is no public health emergency. Because of lack of adequate information-sharing protocols, in nonemergency situations exchange between state public health departments and those involving multiple entities are far more difficult than in emergencies. Unless the patient has clearly given authorization for the exchange to occur, this lack of information more often than not slows or prevents the exchange of data.

Looking at Scenario 16 specifically, we can see that most states have a centralized, secure transfer of information between the state lab contracted to perform newborn screenings and the public health registry. Most public health registries are not open for access to individual physicians; therefore, access is limited to only a small number of public health employees. Although few states explained these systems in detail, the few that did outlined the use of passwords, various levels of access, audits of user activity, and high-level encryption. In 1 state, registry input can be done via the Internet, using a downloadable program installed at the physician's office. The notification of individual patient data between the laboratories and providers, registry and providers, and laboratories/providers and parents is quite variable, however, as mentioned in the discussions of Domains 8 and 9.

For Scenario 17, the data are not kept in a central registry nor is reporting mandated to a central authority; therefore, a wider variety of authorization and access controls was reported for this scenario. For the majority of state teams reporting, these records would be largely paper based; therefore, the inconsistency of authorization and access controls would result in greater restrictions to the exchange of information—restrictions attributable to the sensitive nature of the records being requested. A few states that have electronic billing systems outline requirements such as electronic enrollment into the system and use of user IDs and passwords for submitting electronic patient information. Access roles are also assigned (such as "read only" or "add/modify") according to job requirements. It should be noted, however, that those state teams that discussed electronic systems of this type also mentioned that mental health and substance abuse data were kept separate from a patient's regular health data.

2.10.3 Critical Observations

A variety of critical observations were set forth by the state teams for the public health scenarios. This section discusses those concerns shared by many states, as well as those that were raised by only 1 or 2 states but seemed of particular importance or conveyed strong insight.

Many states mentioned that the use of TB in Scenario 15 made the situation fairly uncomplicated. There are many other types of communicable diseases for which variation in mandatory reporting exists and would create more difficulty for interstate cooperation. A standardization of or agreement on diseases requiring cross-border sharing would be helpful.

Many state teams mentioned that, although processes for dealing with Scenario 15 in particular are fairly straightforward, the ability to verify facts and transmit to or coordinate with other states would be greatly enhanced by the availability of an interoperable electronic clinical information system or registry. One state team also noted that it would be useful to know whom to notify in the sister state, both the health authorities and the law enforcement authorities, and how to notify them outside of business hours. This team indicated that such a system could provide this information.

On the other hand, at least one state team mentioned that its stakeholders felt that personal relationships are often key in transmitting data in a public health emergency, and an electronic system might remove the important human element.

Nearly all state teams mentioned the inability of Medicaid to share data about beneficiaries with other state government programs. This inability often leaves a big hole in immunization and other public health registries. 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. This observation also leads to the general agreement that significant technological barriers to adopting more integrated electronic systems exist among physician groups or clinicians, hospitals, county health departments, and the like.

Many state teams mentioned that the covered entity status of the homeless shelter was debated in reference to Scenario 17. Although the status of the homeless shelter was mentioned in only one state report, it is important to note that the stakeholders felt that not all county health departments are covered entities under HIPAA. HIPAA outlines a path by which public health departments may be excluded as a covered entity; therefore, stakeholders proposed a change to HIPAA to include health departments.

Having a more advanced, centralized system does not remedy all technological issues, however. According to some providers, specific consents for sensitive information create significant difficulties from a technical point of view, because consent is required at every instance of disclosure. Initial technical effort to address the filtering of sensitive information within EHRs, such as genetic information obtained in a newborn screening registry, requires "filtering" logic to check against all available record information that may be transferred. From a consumer advocate point of view, sensitive health information consent requirements provide a high level of privacy protection for sensitive health information. When we look for solutions to this particular issue, a more granular approach to the documentation of consent in different kinds of circumstances might be appropriate for consideration.

State teams also reported the challenges that occur with public health HIEs when they require interstate communications. Examples include a provider in State A seeing a patient from State B and having to report to one or both states, and a provider from the same State B then seeing a patient from State A and having to exchange public health data between agencies across states. The challenges are due to the differences in state law governing reporting, differences in privacy and protection of health information, and disparate business practices.

One state team noted that the business practices related to reporting requirements and gathered from actual public health employees differed much from the practices assumed by non–public health stakeholders, and this difference showed a big gap in understanding. In general, some other state teams found that stakeholders believe there is a lack of transparency around health information disclosures related to public health. Some aspects of public health activities are not covered by HIPAA and do not require an accounting of disclosures. Once involved in a public health situation mandating certain reporting, PHI is shared where necessary, and stakeholders raised examples in which patients were surprised to learn with whom their health information had been shared.

2.11 State Government Oversight (Scenario 18)

18. Health Oversight: Legal Compliance/Government Accountability

The governor's office has expressed concern about compliance with immunization and lead screening requirements among low-income children who do not receive consistent health care. The state agencies responsible for public health, child welfare and protective services, Medicaid services, and education are asked to share identifiable patient-level health care data on an ongoing basis to determine if the children are getting the health care they need. This is not part of a legislative mandate. The governor in this state and those in the surrounding states have discussed sharing this information to determine if patients migrate between states for these services. Because of the complexity of the task, the governor has asked each agency to provide these data to faculty at the state university medical campus who will design a system for integrating and analyzing the data. There is not an existing contract with the state university for services of this nature.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. What is the practice of the organization to provide appropriate information for health care oversight activities? These may include:
   - Determining minimum amount necessary.
   - How to release (electronically or paper—with existing claims data).

2.11.1 Stakeholders

For input on Scenario 18, the majority of state teams gathered data from public health entities, state government officials, and schools that conduct research (Table 2-21). Three of the states did not provide input for this scenario, stating either that it was not relevant to their current landscape or that the stakeholders were unable at this time to provide any feedback on the scenario.

2.11.2 Domains

Note that 4 of the 34 state teams chose to combine their analysis of Scenario 18 with the analysis of Scenarios 15 through 17 (public health; Table 2-22). The breakout of major domains identified by the state teams indicates that not only do the major stakeholders overlap between these 2 scenario groupings, but the major privacy and security domain issues overlap, as well.

Domain 9 (25 out of 34 states): Information Use and Disclosure Policies

Almost all state teams cited the fact that the use of patient-level information outlined in this scenario is typically forbidden without signed patient consent and prior approval by an IRB. The general consensus among state teams was that collected data could not be transmitted from a state health agency to a university without legislative authorization or a data-use-and-sharing agreement. Even though a data-use-and-sharing agreement feasibly could allow disclosure of the data in many states, there is a lack of standard data-sharing agreement and lack of a common language among stakeholders from different states, both of which would compound the problems in sharing data between states.

Table 2-21. Stakeholder Groups Engaged in Scenario 18 Reviews

Stakeholder Group	Number of State Teams Engaging Stakeholder Group in Review of Scenario 18 (N = 34)
Public health agencies	18 (53%)
State government	15 (44%)
Medical and public health schools that undertake research	12 (35%)
Hospitals	6 (18%)
Consumers/consumer organizations	6 (18%)
Community clinics	5 (15%)
Physician groups	4 (12%)
Clinicians	4 (12%)
Payers	4 (12%)
Quality improvement organizations	3 (9%)
Federal health facilities	2 (6%)
Professional associations	2 (6%)
Privacy officers	2 (6%)
Health care attorneys	2 (6%)
Laboratories	1 (3%)
Correctional facilities/law enforcement	1 (3%)
Homecare and hospice	1 (3%)
Long-term care facilities/nursing homes	1 (3%)
RHIOs	1 (3%)

Because of the extreme sensitivities and regulations that would have to be overcome in order for the state health agency to share identified data with the university, many state teams discussed the slightly more realistic goal of just combining data from multiple entities. Although some states have a centralized database to collect this information, many do not. In order to construct a complete picture, data from different agencies would have to be combined, which would pose difficulties because the information was collected with different intentions and permissions. In order to provide patient-identifiable data for secondary public health use, health organizations must have either patient authorization or a legal mandate.

Domain 8 (17 out of 34 states): State Law Restrictions

In states with complex legal structures, an enormous amount of legal analysis taking into account immunization laws, general information privacy laws, and federal and state laws governing the disclosure of information from state agency programs would have to be undertaken to determine whether this data collection was even permissible.

Table 2-22. Nine Privacy and Security Domains Affected by Business Practices Associated With Scenario 18 (N = 34)

State Team	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Alaska									
Arizona							X	X	X
Arkansas		X		X	X		X	X	X
California									X
Colorado				X					X
Connecticut	X	X	X	X	X	X	X	X	X
Florida		X						X	X
Illinois		X		X					X
Indiana[a]								X	X
Iowa[a]		X	X	X	X		X	X	X
Kansas	X	X	X	X	X	X	X	X	X
Kentucky		X					X		X
Louisiana	X	X		X			X	X	X
Maine[a]								X	X
Massachusetts									X
Michigan	X	X	X	X		X	X	X	X
Minnesota									X
Mississippi				X					X
New Hampshire		X							X
New Jersey[a]		X	X	X				X	X
New Mexico			X					X	
New York		X						X	
North Carolina									
Ohio[a]		X		X				X	
Oklahoma	X	X	X	X			X	X	X
Oregon									X
Puerto Rico	X	X	X	X	X	X	X	X	X
Rhode Island									
Utah									
Vermont									
Washington		X					X		X
West Virginia								X	X
Wisconsin	X	X	X	X	X	X	X	X	X
Wyoming									X
Total	7 21%	17 50%	9 26%	15 44%	6 18%	5 15%	12 35%	17 50%	25 74%

Note: Domains of privacy and security are indicated in columns 1–9 as follows: (1) User and Entity Authentication, (2) Authorization and Access Control, (3) Patient and Provider Identification, (4) Transmission Security, (5) Information Protection, (6) Information Audits, (7) Administrative and Physical Safeguards, (8) State Law, and (9) Use and Disclosure Policy. An X indicates that the state team identified at least one business practice affecting that domain. An empty cell indicates that no business practice was identified in association with that domain.

[a] State team combined Public Health Scenarios 15–17 with State Government Oversight Scenario 18.

In a few states with advanced electronic systems, the reporting of immunization data is mandated, but most states have optional reporting. Even states that had advanced systems agreed with most other states, indicating that the action of actually combining data with that from other states would require a legislative mandate.

Domain 2 (17 out of 34 states): Information Authorization and Access Controls

Most state teams that entertained the idea of the exchange (if all other considerations mentioned in Domains 8 and 9 were met) stated that authorization would have to be given by all individuals included in the database, because supposedly the data would be identifiable when transmitted to the university. State teams did discuss some of the issues in Domain 2 that are required for their own state immunization databases (without discussing the issue specifically of supplying these data to other entities or across state lines). In all these systems, users were required to sign confidentiality agreements before gaining access to the information.

Domain 4 (15 out of 34 states): Information Transmission Security or Exchange Protocols

A few states that have advanced electronic immunization and lead screening systems provided guidelines for secure transmission. Transmission of identifiable information from a public health laboratory happens via secure FTP or secure VPN connection. In Michigan the electronic system employs complete role-based access to secure the information. States that theorized the sharing of information between the state agency and the university assumed that this transaction would almost always be electronic. The information would be exchanged via a secure site utilizing public or private encryption keys assigned to users.

2.11.3 Critical Observations

One suggested reason there is such resistance to sharing data electronically is that HIPAA's security regulations require that a covered entity implement procedures to prevent unauthorized access to PHI that is being transmitted (see 45 C.F.R. § 164.312(e)). However, there is no *specific guidance* in the regulations about how to achieve this protection against interception of transmitted information.

HIPAA permits a covered entity to disclose PHI for purposes of data aggregation under a BAA, 45 C.F.R. § 164.504(e); however, in this scenario states are asked to imagine a data aggregation by public health and other government agencies that are not covered entities subject to HIPAA. These agencies are often required by state statute to maintain confidential records, and this fact is seen as problematic to interoperability.

A handful of states also mentioned the Family Education Rights and Privacy Act (FERPA). Even if appropriately strong business agreements could be put in place, FERPA controls all school records, and it has its own privacy and security concerns that are not entirely consistent with HIPAA. Therefore, parents' authorization or consent will likely be required for

the release of the educational record, though there is an exception that may or may not apply to this scenario (34 C.F.R. § 99.31 permits disclosures in cases of health and safety emergency).

One state already maintains an electronic database of immunizations and lead screenings and has contracted to supply these data to universities in the past, although the sharing of data requires an extensive data-use agreement and data are supplied only in de-identified form. Another state is currently considering a system similar to that proposed in the scenario and has encountered major problems with sharing Medicaid data. The proposed alternative is to gather consent from all participants. The Iowa team suggested that states may want to consult the Iowa Medicaid Electronic Records System findings related to barriers encountered during its pilot program, because it involves Medicaid data exchange.

Ultimately, there are many stakeholders who expressed uneasiness about providing information in identifiable form to the university when analysis could be conducted with information in disaggregated form. Although the HIPAA Privacy Rule guides the sharing of information for research purposes, implementation guidelines could differ among organizations. Many state teams felt that the variations in agreements between entities created a chasm that could not easily or quickly be remedied to create an interstate data-sharing program.

3. TEN KEY ISSUES RAISED BY THE STATES IN THE INTERIM ASSESSMENT OF VARIATION

This section briefly describes 10 key issues that were raised by the state teams in the interim reports and that carry broad implications for nationwide electronic health information exchange (eHIE). This section is not intended to be a thorough analysis of the issues or their implications; it serves instead as a descriptive treatment of these issues as they have been identified to date in anticipation of further discussion and analysis by the state project teams (eg, at the national meeting) and by RTI in its final report.

3.1 Misunderstandings and Differing Applications of HIPAA Privacy Rule Requirements

Variation in the application of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provisions often was identified as a barrier to interoperable health data exchange. Many state teams reported broad variation in how the provisions of the HIPAA Privacy Rule are interpreted and applied at the organizational level. This variation in the application of the rules has been identified as a barrier to interoperable eHIE by the majority of state teams.

The state teams report a general lack of understanding about the HIPAA Privacy Rule's premise to generally allow for uses and disclosures of protected health information (PHI) for the core health care purposes of treatment, payment, and health care operations (TPO) (those activities necessary for the health care system to stay in business). This lack of understanding is reflected in the business practices and policies of many of the stakeholder organizations. In some cases, the organizations understand the basic provisions of the HIPAA Privacy Rule but do not have a clear understanding of how and when state law applies. Additional variation is caused by policies developed specifically to be more restrictive than HIPAA in order to reduce the risk of incidental or accidental disclosures. Summarized in this section are some examples from the state teams regarding HIPAA-infused barriers to eHIE.

3.1.1 Consent for Treatment Purposes, Payment, and Health Care Operations

One of the most common issues raised in the state reports was the variability in the use and implementation of patient consent or authorization across organizations. The terms *patient consent* and *patient authorization* are used here interchangeably to refer to the *need for* (perceived or otherwise) and the actual *process of* obtaining appropriate approval from a patient (who is the subject of the information) or a corresponding legal guardian or representative before the disclosure of the health information. Further considerations are as follows:

- HIPAA requires a covered entity to obtain patient authorization (which must adhere to a specific format) for many purposes. HIPAA also specifically permits, but does not require, a covered entity to obtain "consent" for uses and disclosures of PHI for TPO (see 45 C.F.R. § 164.506(b)).
- Many state laws refer to the requirement to obtain patient consent before certain disclosures can occur.
- In the case of HIPAA, the content of the patient authorization is defined and prescribed in detail. In most states, the content of a patient consent form is not defined.

HIPAA does not require patient consent for the use or disclosure of PHI for purposes of TPO, and it is less restrictive than many state privacy laws. Nevertheless, many stakeholders cite HIPAA as the reason for not disclosing information for treatment without patient consent, even in the absence of state law or regulation requiring consent for treatment. In fact, the state teams reported that most stakeholder organizations that participated in this work require patient consent even for treatment purposes.

Four important elements affect the way organizations implement patient consent or patient authorization procedures: (1) federal privacy laws and regulations; (2) state privacy laws and regulations; (3) specific program requirements (such as Medicaid and public health); and (4) additional business practices, policies, and procedures established by organizations, above and beyond what laws and regulations require. Additionally, other factors that affect the ability for health information to be disclosed with or without patient consent or patient authorization include

- who is disclosing the health information,
- what information is being disclosed,
- to whom the information is being disclosed,
- when and how the information will be disclosed,
- who collects the patient consent (the submitter of data vis-à-vis the requester of data), and
- what the purpose of the disclosure is.

Following are the most significant reasons for the reported variability in the interpretation of privacy laws and regulations concerning patient consent or patient authorization.

Lack of understanding about when federal and state laws require patient consent. Most state teams reported consistent disagreement among participating stakeholders about when or why patient consent would be needed.

Lack of a standardized requirement for when to use patient consent. Given the many disclosure scenarios and the variable interpretations of need for patient consent or patient authorization, state teams reported, depending on specifics of each scenario, that

the lack of a uniform approach to need and use of patient consent or patient authorization was causing major barriers to otherwise appropriate and necessary disclosures.

Lack of a standard form to be used in connection with patient consent and authorization. As already noted, the HIPAA Privacy regulations prescribe the content of a HIPAA patient authorization form (used in connection with those disclosures prescribed by HIPAA as requiring a patient authorization), but most states having a patient consent requirement for disclosure offer no definition of what the patient consent "form" is or what the required and optional elements are.

Multiplicity of approaches to the requirement of patient consent. A variety of methods were reported by state teams with respect to the role of consumers in the authorization of HIEs, mainly

- a must all approach, in which patient consent is required in all HIE circumstances;
- an opt-in approach, in which HIE is not permitted unless patient authorizes it;
- an opt-out approach, in which HIE is permitted but patients can choose to not authorize it; and
- a no-opt approach, in which HIE is permitted and patients do not have the ability to opt-out or otherwise stop it.

Variability in the accepted methods to obtain patient consent or patient authorization. There was significant variation in the accepted methods to collect and secure patient consent or authorization. In some circumstances, an e-mail submission was believed sufficient; in others, a faxed form was an acceptable method; and yet in others, a "wet signature" document was required to be on file.

Lack of procedures for when and how to validate or authenticate the patient's authorization or consent. State teams also reported a lack of standard procedures and business practices to confirm a patient's signature on a patient authorization or patient consent. Validity, applicability, and acceptability (legal and otherwise) of digital signatures to support patient consent or patient authorization procedures were in question. The lack of a recognized standard for the use of electronic signatures in conjunction with electronic patient consent or patient authorization forms was highlighted by a number of state teams as a major barrier to automating the process of securing, processing, and storing consents and authorizations. Most states still rely on a "wet signature" to go along with a paper-based patient consent or patient authorization form, even though in most of these states electronic signatures are already recognized as legally acceptable business practices in other industries.

3.1.2 Minimum Necessary

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" (C.F.R. § 164.502(b)). HIPAA requires that uses and disclosures of PHI for anything other than treatment be subjected to *minimum necessary* use review so that no more than the *minimum necessary* amount of information is used or disclosed in each situation. One of the issues surrounding *minimum necessary* is the widespread belief that it applies to disclosures to providers for treatment purposes (even though the HIPAA Privacy Rule explicitly exempts this specific purpose from the *minimum necessary* requirement). Many business practices documented by states show that *minimum necessary* was applied to such disclosures even in emergency-related transfers of records, creating inappropriate barriers to otherwise necessary HIE. This area requires clarification.

A second set of issues involved the inconsistent application of (and lack of models and best practices for) *minimum necessary* in all other non-treatment-related disclosures, including payment, health care operations, public health, health oversight, and judicial and administrative proceedings. What one health care provider may determine to be minimally necessary may vary greatly from another's definition. In addition, several state teams reported that some stakeholder organizations apply the *minimum necessary* standard to internal disclosures and others do not. This variability in the application of the *minimum necessary* standard may present a barrier to information exchange and ultimately to patient care.

A third set of issues is related to burden. Some state teams reported that the federal requirement, in certain types of disclosures, to limit the exchange of health information to the *minimum necessary* standard increases the time required for the exchange and affects the ability to receive comprehensive records. Furthermore, the reports indicated that in many cases technology cannot limit disclosures to the *minimum necessary*, so processes that could be electronic must be manual. For organizations that use paper records, sifting through records to make sure that the *minimum necessary* is exchanged is also time consuming, creating a barrier to exchange.

Other issues highlighted by states included the following:

- the practical applicability of *minimum necessary* for payment-related disclosures (providers reported a tendency to provide payers with whatever information was necessary to obtain payment, generally minimizing the need to make *minimum necessary* determinations, because of limited staff, time, and resources);
- the difficulty of electronic health information systems to make automatic determinations about what constitutes *minimum necessary* without definitions of the right context, purpose for the request, and the like;
- the determination of *minimum necessary* for research-related disclosures; and

- reliance on noncovered entities to request the *minimum necessary* data from providers and others (entities such as public health or health oversight agencies).

The state team reports indicate widespread agreement that current variation in the interpretation and application of the *minimum necessary* standard is a barrier to eHIE and that common understanding of what constitutes *minimum necessary* data sets, as well as who should receive them and under what circumstances, will be required for widespread interoperable eHIE.

3.1.3 Re-release or Redisclosure of PHI Obtained From Another Provider

Although HIPAA does not distinguish the source of PHI except possibly to deny a patient's right to have his or her record amended if it "was not created by the covered entity," some state teams reported confusion about whether the rules for disclosing PHI that had been received from another provider were the same as or different from that generated in-house. Frequently, information that is 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 as to whether a subsequent request for a patient's record should or should not include the information obtained from the other organization. Many organizations reported that they would disclose only patient data that was collected by the organization. In other words, many providers believe that they cannot redisclose another provider's records. On the other hand, some organizations were concerned that sensitive information could be incorporated into the patient's record and then be released downstream without appropriate authorization. Most state teams recognize that the misunderstanding around re-release and redisclosure is a source of variation that will need to be addressed to permit widespread interoperable eHIE.

3.1.4 Importance of Human Judgment Factor in Disclosures

There are several situations in which the HIPAA Privacy Rule calls for "professional judgment" or a "reasonable" decision to be made on the basis of the specific situation. 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 HIPAA's provisions creates an environment where staff interpret disclosure rules restrictively, which sometimes prevents or interrupts HIE, even in treatment situations.

It is important to note here that fear of HIPAA sanctions is not the only source of concern. State teams have reported concern related to federal regulations governing chemical dependency 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 to be a significant source because of the resulting damage to the "brand" of a health care organization. There is no way to "repair" a brand, other than the passage of time. 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 in their approach to 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 exchanging health information has adequately addressed privacy and security issues and minimizes their organization's liability.

3.1.5 Sensitive Information

Although HIPAA considers all PHI sensitive and provides no special treatment for anything except psychotherapy notes, several state teams reported confusion about how to handle "sensitive information" in accordance with a variety of federal and state laws and business practices. For example, concerns addressed

- additional safeguards for highly protected classes of information (HIV, substance abuse, mental health),
- handling of sensitive data,
- state law restrictions on sharing "sensitive" patient information,
- disclosure of sensitive information,
- release of and consent for sensitive health information, and
- requirements for handling of "specialty" records (HIV/AIDS, mental health, substance abuse, genetics).

3.1.6 Accounting of Disclosures

State teams consistently 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. Entities subject to collecting and maintaining information about accountable types of disclosures expressed concerns about the ongoing resources, time, and effort being spent in documenting such disclosures so that, in the event patients or consumers request an accounting of disclosures, they can produce it efficiently and within the time allowed by HIPAA.

The experience reported by providers and others about accounting of disclosures has been that (1) very few patients and consumers have exercised their right to such accounting, and

(2) the type of recorded disclosures is not consistent with what consumers and patients are seeking when they request a copy of the disclosure list. Although this mismatch is not directly a barrier to eHIE, states consistently identified it as an issue that has created confusion and added burden to the process of health information management. The main issues include the following:

- Significant confusion remains regarding 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.
- There is an extremely low level of use of these systems by consumers (the experience has been that only in very rare occasions do consumers request an accounting of disclosures).
- Even when consumers request such accountings, they realize that the disclosures being accounted for are not the ones they are interested in.

3.1.7 General Issues

Most state teams reported consistently that they continue to observe a general lack of understanding about some of the basic tenets of the HIPAA Privacy regulations and of their own state laws concerning the disclosure of health information.

Specifically, states highlighted the following:

- lack of understanding as to whether patient authorization or patient consent is required or not for purposes of TPO, when HIPAA does not require consent or authorization but many state laws actually do;
- lack of understanding of when disclosures not for TPO are permitted without patient consent or patient authorization (such as disclosures to public health, for legal and judiciary proceedings, and for health oversight);
- ambiguity over the distinction between some health care operations (ie, data analysis) and research and the effect of such ambiguity on the ability to disclose the data with or without patient consent or patient authorization;
- variability in the way patient rights are administered across systems, including the rights to request an amendment, the right to request restrictions, and the right to access and obtain a copy of health information;
- issues related to handling information on deceased individuals;
- unclear operational definition of *minimum necessary*, which affects the type and amount of data that are disclosed in a HIE;
- general misconceptions about or unclear definition of ownership of health information;
- lack of standard procedures for handling breaches of privacy, meaning standards that address internal issues with procedures and personnel, as well as external effects on individuals and relationships with other entities; and

- regarding covered entities, as opposed to noncovered entities, limitation of the applicability of HIPAA Privacy regulations to covered entities only and the resulting different standards for health privacy across a region.

The continued lack of understanding (or clarity in definition) around these various issues leads to fear of liability among entities and to conservative applications of HIPAA requirements, consequently creating unnecessary and in some cases inappropriate barriers to eHIE.

3.2 HIPAA Security Rule Misinterpretations and Misunderstandings

A review of state reports indicated some confusion and misunderstanding surrounding what appropriate security practices are, but it also indicated misunderstandings regarding what was currently technically available and scalable to the health care industry and consumers. This lack of knowledge, understanding, and trust between organizations and on the part of consumers was more evident in the business practices than in state laws. For the most part, state laws did not pose challenges to sound security, nor did the HIPAA Security Rule. Sometimes the matter was simply that, even though HIPAA accommodates scalability in security programs, organizations voiced concern related to liability when one organization that believes its security program is more robust sends PHI to another organization with a less robust security program.

There also appeared to be confusion regarding the different types of security required by the HIPAA Security Rule. The Security Rule addresses administrative, physical, and technical security. Even though more than one third of the rule addresses administrative security requirements, many organizations focused more on needed technology than on administrative safeguards.

Following is a series of issues identified during the review and analysis of the state reports. This is a high-level list summarizing what were identified as some of the critical barriers to successful eHIE. Each issue listed is tied to one or more domains (for a detailed description of the 9 domains identified at the beginning of this project by the Agency for Healthcare Research and Quality and the Office of the National Coordinator for Health Information Technology, see Appendix D).

3.2.1 Authentication and Authorization (Domains 1 and 2)

A number of state teams identified the lack of standard authentication and authorization protocols as a barrier to eHIE, especially in more routine settings. Although authentication did not seem to be as great an issue when PHI had to be exchanged for emergency reasons, it did represent a significant barrier to the exchange of PHI for more routine purposes, such as the movement of a patient from one primary care physician to another or the sharing of PHI with a specialist or hospital.

State teams noted that the lack of a common method for authenticating individuals created mistrust between organizations and reduced their comfort level with other organizations' standards or policies regarding who may authorize access to PHI. Most of the concerns were raised about interorganizational exchange of PHI, as opposed to intraorganizational processes for appropriate user authentication methods and standards.

The primary issues relating to authentication and authorization were the lack of standards and interorganizational mistrust. This section will not address the mistrust issues except to state that a commonly accepted set of standards regarding authentication and authorization would go far in alleviating mistrust.

Currently, for authentication some health care entities rely on phone calls or faxes from someone known to that entity while they impose stricter standards on other organizations, including the requirement that the consumer sign an authorization form (although not necessarily required by law) before the PHI is exchanged. It becomes a cumbersome process that does not lend itself well to eHIE.

3.2.2 Inadequate Application-Level Data Access or Screening Controls (Domains 2 and 9)

It is clear from the reports that many stakeholders are not currently using or familiar with currently available technologies. Those stakeholders that are either current users or who are exploring available technologies have identified as another critical issue current inadequacies in existing applications used to manage PHI and used for HIE, including EHRs, data repositories, and the like. For example, some stakeholders indicated that they were required to print out copies of records from EHRs and redact especially sensitive information, or information that should not otherwise be disclosed, because the EHRs did not accommodate segregation of certain types of data. The current business practice is to print a paper copy, redact the information, and fax the redacted copy of the record to the intended recipient.

The perceived technological inadequacy stemming from the inability to appropriately segregate data also was identified as a challenge to appropriate role-based access, or to appropriate management of entities' access, to PHI. 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 reportedly associated with technical inadequacies and led to barriers to allowing external parties electronic access to appropriate portions of the consumer's health record. A number of the states are looking to technology vendors to address these perceived inadequacies.

3.2.3 Audit Programs (Domains 6, 7, and 9)

Several state teams indicated that the current lack of auditing capability because of technical inadequacies and nonexistent or poor audit programs was a challenge to eHIE, particularly when the management of community health records or eHIEs was addressed.

This challenge is especially true when PHI is shared across networks or between 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 PHI. Because community health records and the creation of eHIEs are relatively new, robust standards and related audit log technology have yet to be developed.

Many applications currently in use in the health care industry for the transmission or processing of PHI do not include adequate audit log capability, especially so-called legacy applications (older applications built on what would be considered an outdated software platform). Several state teams raised concerns about the inability to track within their own applications external entities who may have accessed PHI 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.

3.2.4 Secure Transmission of PHI (Domains 4 and 5)

Several state teams identified the secure transmission of PHI between health care organizations, and between health care organizations and consumers, as a significant issue. Reports cited the lack of interoperable solutions and the high cost of implementing appropriate forms of secure transmission that protect the data in transit and protect against inappropriate interception and potential modification. It is more of a technical issue than an administrative security issue.

Concerns raised appear to be related to a lack of understanding of what is currently available on the market and the cost of such solutions. Many vendors serve small to large organizations, as well as consumers, and offer solutions that are scalable, affordable to small to large organizations, and interoperable.

3.2.5 Lack of a Sound Security Infrastructure (All Domains Except 3 and 8)

A number of the state reports addressed interorganizational security issues but did not examine barriers related to these issues (administrative, physical, and technical). Early on,

the Technical Advisory Panel (TAP) noted a significant gap, especially in the provider community, between those organizations that have established sound security programs within their organization and those that have yet to meet the requirements of even the HIPAA Security Rule. Most reports addressed situations in which PHI moves outside their control, as opposed to situations within their control.

The lack of appropriate security program investment by health care and related organizations stems generally from 3 areas that should be reviewed and addressed at the organizational, state, and federal levels:

- lack of knowledge about appropriate security practices and HIPAA rule requirements
- lack of investment in security on the part of the industry (and in some cases government)
- lack of HIPAA Security Rule enforcement by the U.S. Department of Health and Human Services

The fact that most state teams did not specifically address intraorganizational security issues per se demonstrates in part a lack of knowledge of appropriate security standards. The Security Rule is scalable so that small to large organizations can appropriately address what would be considered sound security practices as defined under HIPAA, the National Institute for Standards and Technology, and others. Ultimately, interorganizational security solutions cannot be fully addressed if participants in the eHIE process have not established security programs that adequately protect PHI managed by any one of those participants. The lack of a sound security program represents a weak link in the exchange process.

One of the areas that was addressed by the state teams was the potential cost of implementing appropriate security practices, the lack of infrastructure to support such practices, and other potential technical barriers (such as applications' lacking audit logs, EHRs' lacking the ability to partition data to meet *minimum necessary* standards, and the like). This is an area that must be addressed, even though it is not within the scope of this project. The lack of a sound privacy and security infrastructure in a number of areas, as well as a lack of funding to create one, was a fairly common theme.

3.2.6 Variability in Administrative and Physical Safeguards (Domain 7)

A number of state teams noted that the lack of adoption of consistent and appropriate administrative and physical safeguards within health care organizations has resulted in mistrust between organizations and increased concerns related to liability (where an organization with a sound security program transmits PHI to an organization that lacks a sound security infrastructure). As has been mentioned, a fair portion of what is considered appropriate security falls within the administrative and physical realms.

This issue was noted not as a technology one, but more so one involving lack of understanding about, or insufficient emphasis on, appropriate security for any size

organization. Several state teams noted that such inconsistency resulted in barriers to eHIE and that a good part of the solution would be to address such inconsistencies or inadequate security programs through education and properly understood minimum standards sufficiently flexible to fit the needs of all sizes of health care organizations.

State teams noted that reducing the variability in the application of administrative and physical security would do much to reduce certain challenges to eHIE, improve trust between organizations, and reduce liability concerns. It makes sense that an organization would be more willing to engage in eHIE with another organization if the exchanging organization had a higher comfort level that the recipient had adopted adequate administrative and physical security safeguards.

3.3 Trust in Security

A critical issue raised in many of the state reports was trust as it affects the potential viability of eHIE. Specifically, 2 kinds of stakeholders expressed concerns: consumers and providers. Consumer concerns tended to focus on privacy risks arising 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 arising from the activities of other participants in eHIE and about consumers' lawsuits for inappropriate disclosures of their information; they were secondarily concerned about potential uses of information about consumers by payers and the government.

Review around trust issues was complicated by the fact that critical issues and business practices data were not typically categorized under this heading, and in some cases trust (or lack of it) may have been a motivating but unidentified reason for business practices. There were also a number of cases in which stakeholders other than consumers (eg, providers) articulated their impression that consumer lack of trust was a critical issue, but no consumer data were provided. Ten of the reports lacked information that either expressly or by reasonable inference raised trust as a critical issue.

The leading trust issue was provider fear of lawsuits and liabilities associated with eHIE. 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 HIE. One state identified this as their single most significant issue, one which had been repeatedly raised, and the reason providers were not willing to participate in eHIE. It is not clear whether there is much experiential basis for this fear for most states, but one team identified as a concern a specific statute giving patients a cause of action for inappropriate disclosure, and another reported that HIPAA-based claims are being included in lawsuits by patients frequently enough that one provider had reported 6 such claims within the preceding 6 months. (The

specific legal basis for such claims is not identified. HIPAA does not provide a cause of action for individuals.)

The second most significant trust issue was consumer lack of trust, which appeared to have been expressed directly by consumers in 4 reports and was apparently 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. It appears that one major reason for this lack of trust is the substantial number of security breaches that have been reported over the last few years, including several involving health care organizations.

The most significant general impression that arose from this review was that providers' trust concerns, in particular, appear to be directly correlated with eHIE experience. In other words, providers in states with relatively few eHIE 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 appear not to have such concerns or to have them to a lesser degree.

Finally, one noteworthy finding is that 2 states reported similar reliance on good faith and personal relationships in current practices and identified this reliance as a positive value participants wished to preserve.

3.4 State Laws

The stakeholders identified a number of difficulties with the state laws governing privacy and security, including a general misunderstanding of the intersection of laws and HIPAA, general confusion about where the law was found and how it was applied, and concern that when the law was readily identified and understood it was often too antiquated to apply sensibly to eHIE.

In fact, the leading issue was the absence of state laws clearly applicable to eHIE (sometimes referred to as laws pertaining to RHIOs), which was identified by 11 state teams. Ten state teams identified the generally confusing conditions of state laws as a critical issue, and consistently 11 state teams reported the use of overly conservative business practices due at least in substantial part to confusion or lack of knowledge about state laws. ("Overly conservative" in this context means more restrictive in terms of information-sharing than actually required by law.) At least 2 state teams noted that a number of stakeholders, particularly providers, were unaware of the need to comply with state laws more restrictive than HIPAA and were, in effect, treating HIPAA as a ceiling rather than a floor.

Beyond these general issues, the principal challenges identified involved lack of clarity surrounding the sharing of information with law enforcement (6 state teams), public health

and bioterrorism reports (5 state teams), and confusion about minors' consent (5 state teams). Confusion about genetics laws and electronic signatures was reported by 3 state teams each.

One difficulty in reviewing these reports for state law awareness is identifying state laws that may have been entirely overlooked by the participants. Without independent research, this identification may be difficult or impossible for a reviewer not already familiar with the laws of the state in question, and, although the Legal Working Group should ensure all state law issues are identified, that is not necessarily always the case. For example, Scenario 3 included facts involving execution of an electronic signature. Although almost all states have some form of electronic-signature statute, most have enacted the Uniform Electronic Transactions Act, which was never discussed as a legal issue. Likewise, there was no discussion in any report of the possible implications or barriers raised by practices responsive to the security breach notification statutes now in effect in 17 of the reporting states.

The lack of awareness of and confusion about state laws not only raises risks for eHIE participants, it may also cause them to overlook opportunities such as the liability limitations available under some state digital signature laws (Illinois, Utah, Washington) or useful principles available under other electronic signature laws. (Digital signatures are a specialized form of electronic signature.) Confusion about sharing information for law enforcement, public health, and bioterrorism purposes, in particular, appears to be a critical problem, given concerns about possible bioterror incidents, natural disasters, pandemic flu, and other mass crises. Current practices appear to rely heavily on good will, which is necessary but perhaps not sufficient, especially when interstate coordination is necessary.

The fact that most states' laws are perceived as needing reform may present an opportunity to develop uniform (or at least consistent) eHIE-related state laws. If so, this opportunity should be pursued promptly, since legal reform may be one of the key solutions pursued by many of the reporting states. Unless an effort is made to coordinate such efforts, the various states may implement inconsistent reforms, perhaps resolving some of their own problems but raising new barriers to regional and national interoperation.

3.5 Variations Resulting From Other Federal Laws and Regulations

Although the many applications of HIPAA were cited as a significant source of variation in business practices, it is clear that the interplay of federal regulations that protect sensitive data, state privacy laws, and HIPAA does create confusion for many stakeholders.

3.5.1 42 C.F.R. pt. 2: Federal Substance Abuse Regulations

In the early 1970s, Congress recognized that the stigma associated with substance abuse and fear of prosecution deterred people from entering treatment, so it enacted legislation that gave patients a right to confidentiality. For the almost 3 decades since the federal

confidentiality regulations (42 C.F.R. pt. 2) were issued, confidentiality has been a cornerstone practice for substance abuse treatment programs across the country. These regulations protect all information about any person who has applied for or been given diagnosis or treatment for alcohol or drug abuse at a federally assisted program. 42 C.F.R. pt. 2 generally requires patient permission (authorization) prior to disclosure of information, except in emergency situations. These requirements pose a challenge to the exchange of health information.

There are differences between providers' treatment of patient medical information when substance use is involved. There is variation in the treatment facilities', physicians', and integrated delivery systems' understanding of 42 C.F.R. pt. 2, its relation to HIPAA, and the application of each. Treatment facilities note stringent precautionary measures to safeguard patient substance use information. Physicians comment on limited or restricted access to patient medical files, and treatment facilities note that patient files are kept in a locked cabinet behind a double-locked door.

There is a general understanding of 42 C.F.R. pt. 2 by the treatment facilities responding to the scenarios. However, the differences between the provisions under HIPAA and those under 42 C.F.R. pt. 2 yield a lack of clarity about which regulation applies and under what conditions. The differences in language and drivers for each regulation add to the ambiguity, which increases the variation in how the regulation is applied by organizations.

Lack of understanding about the interaction of HIPAA and 42 C.F.R. pt. 2 implies that, because HIPAA allows sharing of health information for treatment, a provider can share under HIPAA even though sharing without patient authorization would be prohibited under 42 C.F.R. pt. 2.

3.5.2 Clinical Laboratory Improvement Amendments

One state team referred to Clinical Laboratory Improvement Amendments (CLIA) as a barrier to eHIE. CLIA defers to state law for the purpose of determining the permissible recipients of laboratory results. Many state laws very narrowly define those persons who are authorized to receive test results, and variation among state laws has created a medley of different standards.

Under CLIA regulations, 42 C.F.R. § 1291(f) currently states, "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 there is significant uncertainty as to its meaning.

3.5.3 21 C.F.R. § 1306.11

A state team wrote that, regarding Scenario 9, Pharmacy Benefits (A), "federal regulation (21 C.F.R. § 1306.11) which requires that the original written, signed prescription be presented to the pharmacist for review prior to the actual dispensing of the controlled substance represents a barrier to electronic prescription data exchange." This issue was reported to be a potential barrier to eHIE; however, it might be viewed as a security issue that controls dispensing of controlled medication.

3.5.4 Employee Retirement Income Security Act of 1974

One state team noted in relation to Scenario 10, Pharmacy Benefits (B), that "the limit and boundaries of the Employee Retirement Income Security Act, 1974 are not clear" in relation to state law and that this issue will require further consideration as the work progresses.

3.5.5 Family Educational Right to Privacy Act

One state team noted that other highly protective laws like the Family Educational Right to Privacy Act will require consideration as the work progresses, but the team did not explain this comment.

3.6 Networking Issues

This section is included because a number of state teams identified network issues as critical to health information networking and limitations that will result in barriers to eHIE. A common concern across states was the lack of well-defined, operational, and deployable models for regional networking. Significant concerns emerged among the state teams regarding, for example, the legal status of such organizations, their ability to legally operate such eHIEs, and their ability to store and maintain data. There were also concerns about the lack of uniform legal models and business practices for stakeholders to use upon their joining a regional health network. Most state teams reported quite limited interorganizational exchanges of clinical information being done electronically for 3 reasons: (1) lack of implementation of regional networks, (2) limited deployment of EHR systems, and (3) lack of interoperability in those EHR systems that have been deployed. eHIEs between organizations are limited mainly to content-specific clinical messaging in the areas of pharmacy/prescription drug information (e-prescribing), laboratory data, and radiology/digital imaging data.

Significant capacity gaps and variations exist in the levels of resources, technical capabilities, and financial means of organizations (ie, large versus small, urban versus rural). These gaps create significant variation in HIE practices between organizations; in turn, these variations in HIE practices limit or restrict the ability of organizations to conduct interorganizational eHIEs (lack of compatible systems, lack of compatible practices, lack of trust). State teams also noted that different types of eHIE (ie, provider-to-provider,

provider-to-payer, payer-to-payer, and between others) require different handling: some will occur through true message exchanges, some will be done via "pull" mechanism, and others will be achieved with a "push" approach.

States also noted that there is a high comfort level with existing paper-based and manual systems practices and processes for data exchanges. Many expressed the general belief among state participants that current manual practices are timely, are effective, and produce accurate data.

3.7 Linking Data From Multiple Sources to an Individual

The ability for a health care provider to identify the correct records for a patient is critical to clinical medicine and to HIE. The lack of a standard, reliable way of accurately matching records to patients introduces the potential for inappropriate use or disclosure of PHI from the wrong patient, which is both a clinical and a privacy risk. This risk is particularly acute in the case of information shared across institutions where the methods of patient and record identification in one differ from those in the other.

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 HIEs 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 eHIE 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.

Unique patient and provider identification was also discussed as part of the overall review of critical *security* issues (see Section 3.3, Trust in Security). Being able appropriately to identify patients and providers is not only critical in the delivery of quality care to patients

and for the exchange of heath information, but also is a fundamental issue in other information security domains, such as authentication and authorization.

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 eHIEs are conducted were perceived as major challenges by many state teams. 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, or NPI). Providers, payers, and others are required to fully implement the NPI by May 23, 2007.

3.7.1 Types of Patient Identification Used

Current practices reported by participating stakeholders from most states pointed at 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.

Given the lack of a national (or state) unique patient identifier, several alternatives were discussed by state teams 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 where health information about that individual exists.

Other mechanisms considered varied from the creation of a regional Master Patient Index, 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.

Most state teams also highlighted the need to establish these standard mechanisms to uniquely identify patients across organizations as a foundational component of the evolving eHIEs.

3.7.2 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 (public health functions); 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 in order 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 in order to access the information accurately and reliably.

Consumer-related challenges included the fact that consumers with health information residing at various organizations and in various systems are required to maintain different types of identifiers to access their information reliably.

3.7.3 Patient Identification: Consumer Communication and Education

Many state teams noted the need to engage consumers early and throughout the process of establishing such unique patient identification approaches to help them buy into the proposed approaches, as well as support any legislative and funding initiative necessary to support the implementation of the proposed methods.

The state teams were acutely aware of the potential increase in risk of privacy violations and identity theft, a risk increase brought about by any attempt to implement a unique patient ID across institutions or regions, and they were aware of the need to counter possible negative public reaction with effective security controls and extensive consumer education.

3.8 Interstate Issues

Although the identification of interstate issues was not a primary focus of the interim assessment of variation, 16 state teams reported that interstate issues should be considered carefully, although it is not clear that the issues cited posed critical barriers to eHIE. Interstate issues were typically raised by states for 3 reasons: (1) they had considerable sharing of health care information across state lines; (2) when the state experiences very large seasonal inflows of both out-of-state workers and tourists, its residents make substantial use of out-of-state providers; and (3) a number of interstate

health systems and plans have facilities and do business in the state. One markedly rural state noted that, because of its relative paucity of certain types of health care facility, access to other states' hospitals and specialty services is crucial for its residents: any meaningful health information infrastructure would have to reach major metropolitan areas in 3 other states.

The legal variations noted as potential barriers to eHIE include differences in standards for genetic information; electronic prescriptions; immunization, HIV/AIDS, and minors' rights; minors' consents; workers' compensation; and mental health and substance abuse. In addition to interstate issues, at least one state team reported that variations between state and American Indian tribal standards were critical to developing statewide eHIEs. Several states noted that they did not believe interstate issues to be problematic and indicated that the disclosing state's law generally controlled. Most issues were between organizations rather than between states, and interstate issues tended to be resolved within organizations.

It is worth noting that no state identified variations in security breach notification laws as an issue. This is, in fact, an important issue that has emerged in the past 2 or 3 years. Security breach notification laws have been adopted in at least 26 states, including 17 of the states reporting and 14 states adjacent to reporting states. The application of a state's law is triggered by a security incident, in electronic form, affecting health information about residents of the state, wherever the incident occurs. Organizations in states without security breach statutes are required to notify residents of other states with such laws if information about them has been affected. For example, in a notorious incident last year, the multistate Providence Health System experienced a security incident when electronic media were stolen in Portland, Oregon. Although Oregon does not have a security incident law, the organization was required to notify residents in several states that did, including adjacent Washington.

3.9 Disclosure of PHI

The ability of one entity to disclose health information to another is at the core of the implementation of interoperable eHIEs. Several federal and state laws and regulations, as well as specific program requirements, affect both whether or not specific disclosures can take place and also the way such disclosures can be achieved. Overall, state teams consistently identified the variation in business practices related to the disclosure of health information as a significant set of factors affecting the ability to conduct eHIE between organizations.

3.9.1 Interpretation of Requirements for the Re-release or Redisclosure of Health Information

One of the common challenges identified by state teams was the variability in the understanding of when health information can be re-released or redisclosed by an entity that received the information from another entity. Although this issue runs across several scenarios, it was particularly noted concerning sensitive health information, such as mental health or substance abuse records. It was also of special concern with data crossing state lines.

The current paper environment was mentioned by some states as more conducive to preventing "unintended" redisclosures than a future EHR environment, although in other states the electronic environment was noted as capable of more effectively controlling which information could be disclosed and which could not.

3.9.2 Differences in How Sensitive Health Information Must Be Treated

Almost all states highlighted as a major concern the differences in how certain health information (generally considered more sensitive than other types) must be specially handled when one is disclosing such information. In particular, the variability in the understanding, interpretation, and implementation of federal and state laws and program requirements results in more stringent protections to these data.

One of the concerns noted by state teams was the creation of a dual standard for handling health information: the "basic" one for all health information not considered relatively sensitive, and a more stringent set of requirements for specific health information considered to be sensitive. Examples of sensitive data include

- data about minors,
- data concerning reproduction,
- data about communicable diseases,
- data about sexually transmitted diseases,
- HIV/AIDS data,
- mental health data,
- chemical dependency data,
- genetic information,
- prescription drug information (when it may lead to the disclosure of a sensitive condition), and
- abuse and neglect exposure.

In some cases, the additional requirements imposed on this type of data create the need to implement dual or separate patient consents, "per instance" consents when recurring

disclosures are going to be needed, or even special re-release consents when a second provider is making the disclosure.

Other issues and concerns expressed regarding sensitive health information involved determinations about what is "sensitive" health information; usually "sensitive" ends up being defined by the provider on the basis of his or her understanding of the rule and the type of data being disclosed. Concerns about interstate exchange of sensitive information also abound; there are differences across states on how sensitive information must be handled, differences which create additional issues for the entity that is disclosing the data.

3.9.3 Issues of Ownership of Health Information

State reports also identified the lack of a clear and consistent definition of ownership of health information (and the variability in the interpretations of "who owns the data") as a challenge to eHIE.

Most state teams reported that the HIPAA Privacy regulations did not provide such definition of ownership and that state laws also lacked any specific references to the issue. Nevertheless, some state teams did identify specific state laws that defined ownership of medical records, although in many cases the state laws identified the provider who generated the record as the owner of the record while in other states the individual was considered to be the owner of the record.

3.9.4 Need for Fast, Easy, and Secure eHIE Under Medical or Health Emergency Circumstances

One subject about which there was consensus among state teams was the need to ensure that under emergency circumstances health information will be able to be exchanged quickly, easily, and securely between and across providers, as well as across state borders. In the description of business practices related to the emergency circumstances scenario, many state teams noted that there was some confusion about when, how, and by whom a patient consent or patient authorization must be solicited in order for an entity to receive health information about the patient from other providers. There were also concerns expressed about what would be the minimum amount of data that should be exchanged in emergency situations, or whether all data should be accessible and available.

Additional concerns included specific state laws that might restrict the disclosure of certain (sensitive) information even in emergency situations without a proper patient consent and patient authorization, and challenges attributable to exchange of data across state borders when different state laws and regulations apply.

3.9.5 Variations in Interpretation of Reporting Requirements for Public Health Purposes

When dealing with reporting of health information to public health agencies (and other health oversight agencies), states reported the following issues:

- Most participating stakeholders were able to identify appropriate and relevant state laws that required and defined the parameters under which specific disclosures of health information to public health must be performed.
- Stakeholders also noted a lack of standardized rules for all public health entities across states when they were requesting access to patient information. Some states may be reluctant to disclose patient health information to states that have lesser privacy protections.
- There are many types of public health notification requirements, and issues such as *minimum necessary* apply to such disclosures, but there are no consistent mechanisms by which public health authorities may determine the *minimum necessary* information, an element providers must rely upon before making such disclosures.
- Entities have difficulty identifying and relating to the multiplicity of layers of public health laws and regulations covering the release of health information.
- Many reported that they tend to not disclose information for fear of being sanctioned for a particular privacy law that they were not fully aware of or did not understand appropriately.
- Covered entities expressed concerns about their providing health information that is protected by HIPAA, but losing control over the privacy and security of the same information once it is released to a noncovered public health entity.
- Many participating stakeholders reported a lack of trust in public health agencies because of lack of transparency around health information disclosures related to public health.

3.9.6 Handling of Disclosures Related to Judicial Proceedings and Law Enforcement

The disclosure of health information in instances in which judicial proceedings and law enforcement are involved was also reported to have some variations in terms of when such disclosures may occur, how they can be achieved, what specific requirements must be met in order for providers and others to be able to make the disclosure, and whether or not there is a need for a patient consent or patient authorization to perform such disclosures (even though HIPAA Privacy regulations permit such disclosures, subject to certain conditions, without patient authorization).

In most cases cited by state teams, the determination of whether a particular disclosure could be made to law enforcement followed strict parameters and business practices. Most states also had laws that required either patient consent or a court order for such disclosures. The issues identified by states related to whether front-line staff dealing with

such situations were appropriately trained on the implementation of the business policies and procedures established by the organization for this type of disclosure.

3.10 Cultural and Business Issues

State teams referenced a number of business issues that pose challenges to the electronic exchange of health information. 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. Many state teams reported that their state's patient consent requirements place responsibility and liability for the appropriate release of patients' health information on the health care provider *releasing* information and place no responsibility on health care providers *requesting* the information.

Another example of a business issue that poses a challenge is general resistance to change, which is a common issue that organizations face whenever there is a change in how business is conducted. This issue is frequently cited as a cultural issue in discussions about decisions to adopt electronic systems. There is a certain comfort with existing paper-based or manual systems and data exchange practices and processes, and there is a general belief that current manual practices are timely, effective, and productive of accurate data. Implicit in some of the discussions is an assumption that security slows down the process, in the sense that the data are secure but access is not as fast as a phone call away. In fact, person to person is how most exchanges take place, especially in emergency situations, and human judgment plays a large role in how and when information is exchanged. A number of states have noted that the current system is based on trusted person-to-person exchanges. Many state teams have noted that it will be important to include the points at which human judgment is required in the specifications for any safe system developed to exchange information electronically.

As mentioned earlier in this report, a third 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 serve to increase variation as organizations attempt to meet compliance by defining terms in ways that protect the interests of the organization.

Another cultural issue that state teams have raised involves the tension between health care providers, hospitals, and patients concerning who controls or owns the data. A number of providers indicated that they did not think that patients should have full access to their records, especially to doctors' notes. There was a concern that doctors would not enter complete notes if the patient would be able to access the record. There were also concerns about liability. However, the majority of stakeholders agreed that there is a need to address

patients' needs, interests, and concerns and that doing so is critical to the success of interoperable eHIE.

APPENDIX A
LIST OF STAKEHOLDERS[3]

- Clinicians
- Physician groups (primary and specialty care)
- Federal health facilities (Department of Health, Indian Health Service, Department of Veterans Affairs)
- Hospital personnel/ER staff
- Payers
- Public health agencies
- Community clinics and health centers
- Laboratories
- Pharmacies
- Long-term care facilities/nursing homes
- Homecare and hospice
- Correctional facilities personnel
- Professional associations and societies
- Medical and public health schools that undertake research
- Quality improvement organizations
- Consumers/consumer organizations
- State government (Medicaid, public health departments, etc)

[3] This is the stakeholder list described on page 49 of AHRQ-05-0115 request for proposal dated June 7, 2005.

APPENDIX B
PRIVACY AND SECURITY HEALTH INFORMATION EXCHANGE SCENARIOS GUIDE

The following 18 scenarios were developed specifically for the privacy and security project to provide a standardized context for discussing organization-level business practices across all states and territories. The scenarios represent a wide range of purposes for the exchange of health information (eg, treatment, public health, biosurveillance, payment, research, and marketing) across a broad array of organizations involved in health information exchange and actors within those organizations. The product of the "guided or focused" discussions will be a database of organization-level business practices that will form the basis for the assessment of variation upon which all other work will be based.

Each scenario describes a *health information exchange* within a given context to ensure that we cover most of the areas in which we expect to find variation. Clearly, the scenarios do not cover the universe of exchanges—which would be impossible, given the time frame for the project. However, the purposes and conditions represented in the scenarios will generate discussions in the key areas where we can expect to find business practices, policies, and state laws that impact interoperable health information exchange and will serve as the catalyst for further discussions as the project moves forward.

Key to the success of using the scenarios is bringing the appropriate stakeholders together to discuss the appropriate scenarios. Figure B-1 shows a mapping of the relevant stakeholder organizations to the 18 scenarios. A darker shaded box containing an "X" provides a text description of the primary stakeholders identified in each scenario. These primary stakeholders are most likely to be knowledgeable about the business practices and policies that their specific organization engages in, given the situation presented in the scenario, and should be invited to discussions of those specific scenarios. A yellow shaded box with no text indicates a secondary stakeholder group that could conceivably weigh in on the discussions generated by that scenario. For example, Scenario 1, Patient Care Scenario A, involves an exchange between the ER in Hospital A and an out-of-state hospital, Hospital B. Both the requesting and disclosing organizations are hospitals, regardless of the "actors" that may be representing those organizations in the work group meetings, which may include physicians, nurses, health information management professionals, and others. The organizations that are relevant for each scenario are also identified at the beginning of each scenario to facilitate the coordination of stakeholders for each work group.

Figure B-1. Scenario by Stakeholder Map

Scenarios	1. Clinicians	2. Physician groups	3. Federal health facilities	4. Hospitals	5. Payers	6. Public Health agencies	7. Community clinics and health centers	8. Laboratories	9. Pharmacies	10. Long-term care facilities and nursing homes	11. Homecare and hospice	12. Law enforcement/ correctional facilities	13. Professional associations and socieities	14. Medical and public health schools that undertake research	15. Quality improvement organizations	16. Consumers or consumer organizations	17. State government (Medicaid, public health departments)	18. Other, specify
1. Patient Care - Scenario A (Emergent Transfer)				X ER Staff (sending and receiving)														
2. Patient Care - Scenario B (Sub Abuse)	X Provider	X Primary Care Physician					X Substance Abuse Treatment									X Client/Patient		
3. Patient Care - Scenario C (Access Security)	X Provider	X Psychiatrist		X Hospital Psych Unit						X Nursing Facility								X Transcription Service
4. Patient Care - Scenario D (HIV and Genetic)				X Mamography Dept.			X Outpatient Clinic											
5. Payment Scenario	X Provider	X Provider	X Provider	X Provider	X Health Plan		X Provider			X Provider	X Provider					X Patient		
6. RHIO Scenario	X Provider	X Provider	X Provider	X Provider			X Provider	X Provider	X Provider	X Provider	X Provider							
7. Research Final Scenario	X Provider	X Provider												X IRB, Research Investigator		X Study Member		
8. Law Enforcement Final Scenario				X Provider								X Law Enforcement				X Patient Patient's family		
9. Pharmacy Benefit Final Scenario A							X Outpatient Clinic		X Pharmacy Benefit Manager							X Patient		
10. Pharmacy Benefit Final Scenario B									X Pharmacy Benefit Manager							X Employees		X Company
11. Operations and Marketing Final Scenario A				X Tertiary Hospital Marketing Dept			X Critical access clinics (sending)											
12. Operations and Marketing Final Scenario B				X Obstetrics department Marketing												X Patient		X Company
13. Bioterrorism Event Final Scenario	X Provider	X Provider		X Provider		X Public Health Staff						X Law Enforcement					X Emergency Gov't agencies	
14. Employment Information Final Scenario				X ER Staff												X Employees		X Company HR Dept
15. Public Health Final Scenario A	X Provider	X PCP				X Public Health Staff						X Law Enforcement				X Patient		
16. Public Health Final Scenario B	X Provider	X Physician				X Public Health Staff	X Specialty Care Center	X Lab Staff									X Public Health	
17. Public Health Final Scenario C	X Provider	X PCP		X Drug Treatment Center			X Homeless shelter Community									X Patient Patient's family	X County Program	
18. Health Oversight Final Scenario						X Public Health Staff								X Faculty				

Health Information Exchange Scenarios

1. Patient Care Scenario A

The emergent transfer of health information between two hospitals that represent the 2 stakeholder organizations (ie, Hospital A and Hospital B) when the status of the patient is unsure. The actors are the staff involved in carrying out the request. The ER physician is requesting the information on behalf of Hospital A.

Stakeholder organizations and exchanges:

- Hospital emergency room in Hospital A is the organization requesting information.
- Hospital B is the organization releasing the information.

Patient X presents to emergency room of General Hospital in State A. She has been in a serious car accident. The patient is an 89-year-old widow who appears very confused. Law enforcement personnel in the emergency room investigating the accident indicate that the patient was driving. There are questions concerning her possible impairment due to medications. Her adult daughter informed the ER staff that her mother has recently undergone treatment at a hospital in a neighboring state and has a prescription for an antipsychotic drug. The emergency room physician determines there is a need to obtain information about Patient X's prior diagnosis and treatment during the previous inpatient stay.

Potential areas for discussion of BUSINESS PRACTICES based on this scenario:

1. Determining status of the patient and chain of responsibility.
2. Practice and policy for obtaining information sufficient for treatment.
3. Practice and policy for handling mental health information.
4. Practice and policy for securing the data exchange mechanism.
5. Practice and policy related to authentication of requesting facility by the releasing facility.
6. Practice and policy related to patient authorization for the release of information.

2. Patient Care Scenario B

The scenario involves the nonemergent transfer of records from a specialty substance treatment provider to a primary care facility for a referral to a specialist.

Stakeholder organizations and exchanges:

- Specialty substance abuse treatment facility (releasing sensitive clinical records)
- Primary care provider's organization (eg, doctor's office, community health center, public health agency) (requesting clinical records from the substance abuse facility, releasing information to specialist)

An inpatient specialty substance abuse treatment facility intends to refer client X to a primary care facility for a suspected medical problem. The 2 organizations do not have a previous relationship. The client has a long history of using various drugs and alcohol that is relevant for medical diagnosis. The primary care provider has requested that the substance abuse information be sent by the treatment facility. The primary care provider intends to refer the patient to a specialist and plans to send all of the patient's medical information, including the substance abuse information that was received from the substance abuse treatment facility, to the specialist.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. How does the releasing organization obtain authorization from the patient to allow release of medical records?
2. What is the process for handling substance abuse medical record data?
3. How does the releasing organization authenticate the health care provider requesting the information?
4. How is the data exchange secured?

3. Patient Care Scenario C

Stakeholder organizations and exchanges:

- Hospital psychiatric unit (sending) and the skilled nursing facility (receiving)
- Physician (sending) and the transcription service (receiving)
- Transcription service (sending) and the physician (receiving)
- Physician (sending) and the skilled nursing facility (receiving)

At 5:30 p.m., Dr. X, a psychiatrist, arrives at the skilled nursing facility to evaluate his patient, recently discharged from the hospital psychiatric unit to the skilled nursing facility. The hospital and skilled nursing facility are separate entities and do not share electronic record systems. At the time of the patient's transfer, the discharge summary and other pertinent records and forms were electronically transmitted to the skilled nursing home.

When Dr. X enters the facility, he seeks assistance locating his patient, gaining entrance to the locked psychiatric unit, and accessing the patient's electronic health record to review the discharge summary, I&O, MAR, and progress notes. Dr. X was able to enter the unit by showing a picture identification badge, but was not able to access the EHR. As it is Dr. X's first visit, he has no log-in or password to use their system.

Dr. X completes his visit and prepares to complete his documentation for the nursing home. Unable to access the skilled nursing facility EHR, Dr. X dictates his initial assessment via telephone to his outsourced, offshore transcription service. The assessment is transcribed and posted to a secure Web portal.

The next morning, from his home computer, Dr. X checks his e-mail and receives notification that the assessment is available. Dr. X logs into his office Web portal, reviews the assessment, and applies his electronic signature.

Later that day, Dr. X's office manager downloads this assessment from the Web portal, saves the document in the patient's record in his office, and forwards the now encrypted document to the long-term care facility via e-mail.

The skilled nursing facility notifies Dr. X's office that they are unable to open the encrypted document because they do not have the encryption key.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Agreements for data sharing—business associate agreements.
2. Setting out access and role management policies and practices for temporary or new access.
3. Determining appropriate access to mental health records.
4. Securing unstructured, possibly nonelectronic patient data.
5. Reliability of other entity security and privacy infrastructure.

4. Patient Care Scenario D

The nonemergent transfer of health information

Stakeholder organizations and exchanges:

- Hospital mammography department (requesting health information)
- Outpatient clinic (receiving request)

Patient X is HIV positive and is having a complete physical and an outpatient mammogram done in the Women's Imaging Center of General Hospital in State A. She had her last physical and mammogram in an outpatient clinic in a neighboring state. Her physician in State A is requesting a copy of her complete records and the radiologist at General Hospital would like to review the digital images of the mammogram performed at the outpatient clinic in State B for comparison purposes. She also is having a test for the *BrCa* gene and is requesting the genetic test results of her deceased aunt who had a history of breast cancer.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Authenticating entities and individuals.
2. Determining processes and laws for release of genetic and HIV information.

5. Payment Scenario

Stakeholder organizations and exchanges:

- Health care provider (hospital or clinic)
- Health plan (payer)
- Patients

X Health Payer (third party, disability insurance, employee assistance programs) provides health insurance coverage to many subscribers in the region the health care provider serves. As part of the insurance coverage, it is necessary for the health plan case managers to approve/authorize all inpatient encounters. This requires access to the patient health information (eg, emergency department records, clinic notes).

The health care provider has recently implemented an electronic health record (EHR) system. All patient information is now maintained in the EHR and is accessible to users who have been granted access through an approval process. Access to the EHR has been restricted to the health care provider's workforce members and medical staff members and their office staff.

X Health Payer is requesting access to the EHR for their accredited case management staff to approve/authorize inpatient encounters.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Get patient authorization to allow payer access.
2. Facility needs to determine the minimum necessary and limit to pertinent time frame.
3. If allowed, access and role management are issues.
4. Determine method for enabling secure remote access if allowed.

6. RHIO Scenario

Note: Each stakeholder should participate in this scenario keeping in mind the type of data their organization anticipates exchanging with an RHIO.

Stakeholder organizations and exchanges:

- Multiple provider organizations (providing data)
- Multiple RHIOs (receiving data)

The RHIO in your region wants to access patient identifiable data from all participating organizations (and their patients) to monitor the incidence and management of diabetic patients. The RHIO also intends to monitor participating providers to rank them for the provision of preventive services to their diabetic patients.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Decision to utilize medical record data to monitor disease management.
2. Authorization from patients to allow RHIO to monitor their PHI for disease management.
3. Determine mode of transferring information and type of information, ie, identifiable or de-identified information to the RHIO.

7. Research Data Use Scenario

Stakeholder organizations and exchanges:

- Health care consumer (taking part in the study)
- Health care provider (distributing meds and collecting clinical data)
- Research investigator (receiving and analyzing clinical data)
- Institutional Review Board (IRB) (receiving reports on data collection)

A research project on children younger than age 13 is being conducted in a double-blind study for a new drug for ADD/ADHD. The research is being sponsored by a major drug manufacturer conducting a double-blind study approved by the medical center's IRB, where the research investigators are located. The data being collected is all electronic, and all responses from the subjects are completed electronically on the same centralized and shared database file.

The principal investigator was asked by one of the investigators if they could use the raw data to extend the tracking of the patients over an additional 6 months or use the raw data collected for a white paper that is not part of the research protocols final document for his postdoctoral fellow program.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. IRB approval of any significant changes to the research protocol.
2. Research subjects have signed consents and authorization to participate in the research effort.

8. Scenario for Access by Law Enforcement

Stakeholder organizations and exchanges:

- Health care provider (providing health information)
- Law enforcement
- Patient
- Patient's family

An injured 19-year-old college student is brought to the ER following an automobile accident. It is standard to run blood-alcohol and drug screens. The police officer investigating the accident arrives in the ER, claiming that the patient may have caused the accident. The patient's parents arrive shortly afterward. The police officer requests a copy of the blood-alcohol test results, and the parents want to review the ER record and lab results to see if their child tested positive for drugs. These requests to print directly from the electronic health record are made to the ER staff.

The patient is covered under his parent's health and auto insurance policy.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. County contracts with emergency department to perform blood-alcohol test draws.
2. Printing of additional copies of medical record reports for parents, insurance companies, and police.
3. Asking patient if it is okay to talk to parents or give information to parents about their condition.
4. Communication with primary care provider.

9. Pharmacy Benefit Scenario A

Stakeholder organizations and exchanges:

- Pharmacy benefit manager (PBM) (requesting information)
- Outpatient clinic (receiving request)
- Patient X

The PBM has a mail order pharmacy for a hospital which is self-insured and also has a closed formulary. The PBM receives a prescription from Patient X, an employee of the hospital, for the antipsychotic medication Geodon. The PBM's preferred alternatives for antipsychotics are Risperidone (Risperdal), Quetiapine (Seroquel), and Aripiprazole (Abilify). Since Geodon is not on the preferred alternatives list, the PBM sends a request to the prescribing physician to complete a prior authorization in order to fill and pay for the Geodon prescription. The PBM is in a different state than the provider's outpatient clinic.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Patient authorization to share information with the PBM.
2. Agreements for data sharing—business associate agreements.
3. Health care provider must determine minimum necessary access to PHI.
4. If allowed, role and access management are issues.
5. Determine method for enabling secure remote access if allowed.

10. Pharmacy Benefit Scenario B

Stakeholder organizations and exchanges:

- Pharmacy benefit manager (PBM) (requesting information)
- Company A (providing claims information)
- Employees

A PBM (PBM1) has an agreement with Company A to review the companies' employees' prescription drug use and the associated costs of the drugs prescribed. The objective would be to see if PBM1 could save the company money on their prescription drug benefit. Company A is self-insured and as part of their current benefits package, they have the prescription drug claims submitted through their current PBM (PBM2). PBM1 has requested that Company A send their electronic claims to them to complete the review.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Business associate agreements and formal contracts exist between Company A and the PBMs.
2. The extent and amount of information shared between the various parties would be limited by the minimum necessary guidelines.

11. Health Care Operations and Marketing Scenario A

Note: This scenario could be modified to apply to any health care provider (physician group, home health care agency, etc.) wishing to market services to a targeted subset of patients.

Stakeholder organizations and exchanges:

- Tertiary hospital (requesting study data)
- Critical access hospital (being asked to provide health information)

ABC Health Care is an integrated health delivery system composed of ten critical access hospitals and one large tertiary hospital, DEF Medical Center, which has served as the system's primary referral center. Recently, DEF Medical Center has expanded its rehab services and created a state-of-the-art, stand-alone rehab center. Six months into operation, ABC Health Care does not feel that the rehab center is being fully utilized and is questioning the lack of rehab referrals from the critical access hospitals.

ABC Health Care has requested that its critical access hospitals submit monthly reports containing patient identifiable data to the system six-sigma team to analyze patient encounters and trends for the following rehab diagnoses/procedures:

- Cerebrovascular accident (CVA)
- Hip fracture
- Total joint replacement

Additionally, ABC Health Care is requesting that this same information, along with individual patient demographic information, be provided to the system Marketing Department. The Marketing Department plans to distribute to these individuals a brochure highlighting the new rehab center and the enhanced services available.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Decision to conduct marketing using PHI with their consumers.
2. Authorization from consumer to allow IHDS to market to themselves.
3. Determine mode of transferring information and type of information, ie, identifiable or de-identified information to the marketing department

12. Health Care Operations and Marketing Scenario B

Stakeholder organizations and exchanges:

- Health care provider (hospital obstetrics department sending data)
- Hospital marketing department (receiving data)
- Local company (purchasing data from marketing department)
- Patients/consumers

ABC hospital has approximately 3,600 births per year. The hospital marketing department is requesting identifiable data on all deliveries, including mother's demographic information and birth outcome (to ensure that contact is made only with those deliveries resulting in healthy live births).

The marketing department has explained that they will use the patient information for the following purposes:

1. To provide information on the hospital's new pediatric wing/services.
2. To solicit registration for the hospital's parenting classes.
3. To request donations for construction of the proposed neonatal intensive care unit.
4. To sell the data to a local diaper company to use in marketing diaper services directly to parents.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Requesting patient consent or permission to use and sell identifiable data for marketing purposes.
2. Decisions to conduct marketing using patient data.
3. Determining mode of transferring information and type of information, ie, identifiable or de-identified information to the marketing department.

13. Bioterrorism Event

Stakeholder organizations and exchanges:

- Laboratory (collecting data)
- Health care provider (transmitting data to public health)
- Public health department (receiving data from provider, providing data to government agencies)
- Law enforcement (receiving data)
- Government agencies (receiving data)
- Patients

A provider sees a person who has anthrax, as determined through lab tests. The lab submits a report on this case to the local public health department and notifies their organizational patient safety officer. The public health department in the adjacent county has been contacted and has confirmed that it is also seeing anthrax cases, and therefore this could be a possible bioterrorism event. Further investigation confirms that this is a bioterrorism event, and the state declares an emergency. This then shifts responsibility to a designated state authority to oversee and coordinate a response, and involves alerting law enforcement, hospitals, hazmat teams, and other partners, as well as informing the regional media to alert the public to symptoms and seeking treatment if feeling affected. The state also notifies the federal government of the event, and some federal agencies may have direct involvement in the event. All parties may need to be notified of specific identifiable demographic and medical details of each case as it arises to identify the source of the anthrax, locate and prosecute the parties responsible for distributing the anthrax, and protect the public from further infection.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Providing patient-specific information related to specific symptoms to law enforcement, CDC, Homeland Security, and health department in a situation where a threat is being investigated.

14. Employee Health Information Scenario

Stakeholder organizations and exchanges:

- Hospital emergency room (releasing health information)
- Employer human resources department (requesting health information)
- Employee

An employee (of any company) presents in the local emergency department for treatment of a chronic condition that has worsened but is not work related. The employee's condition necessitates a 4-day leave from work for illness. The employer requires a "return to work" document for any illness requiring more than 2 days leave. The hospital Emergency Department has an EHR and their practice is to cut and paste patient information directly from the EHR and transmit the information via e-mail to the Human Resources department of the patient's employer.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Determining employee agreement to release information.
2. Determining what are the minimum necessary elements which can be legally transmitted.
3. Ensuring the data is secured as it is transmitted.

15. Public Health Scenario A—Active Carrier, Communicable Disease Notification

Stakeholder organizations and exchanges:

- Health care provider (primary care physician)
- Public health department
- Law enforcement
- Patient

A patient with active TB, still under treatment, has decided to move to a desert community that focuses on spiritual healing, without informing his physician. The TB is classified MDR (multidrug resistant). The patient purchases a bus ticket—the bus ride will take a total of 9 hours with 2 rest stops across several states. State A is made aware of the patient's intent 2 hours after the bus with the patient leaves. State A now needs to contact the bus company and other states with the relevant information.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Providing patient-specific information related to a specific communicable disease to law enforcement, non–health care entities, and health department in a situation where a threat is being responded to.
2. Ensuring the data is secured as it is transmitted.

16. Public Health Scenario B—Newborn Screening

Stakeholder organizations and exchanges:

- Health care provider (sending initial data to public heath and lab, receiving data on follow up/eligibility)
- State laboratory (receiving data)
- State public health department (receiving data, sending data for program eligibility)

A newborn's screening test comes up positive for a state-mandated screening test and the state lab test results are made available to the child's physicians and specialty care centers specializing in the disorder via an Interactive Voice Response (IVR) system. The state lab also enters the information in its registry, and tracks the child over time through the child's physicians. The state public health department provides services for this disorder and notifies the physician that the child is eligible for those programs.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. Providing patient-specific information related to specific symptoms of a disease to a health department in a situation where a targeted disease is being investigated.

17. Public Health Scenario C—Homeless Shelters

Stakeholder organizations and exchanges:

- Primary care provider (sending) and hospital-affiliated drug treatment center (receiving)
- The hospital-affiliated drug treatment clinic (releasing) and the county program (requesting for purposes of reimbursement)
- The hospital-affiliated drug treatment clinic (releasing) and the shelter (requesting to verify the treatment)
- The family member (requesting) and the shelter

Stakeholder entities:

- Health care consumer/patient
- Primary care provider
- Hospital-affiliated drug treatment center
- Homeless shelter
- Patient relative/family member

A homeless man arrives at a county shelter and is found to be a drug addict and in need of medical care. The person does have a primary care provider, and he is sent there for medical care. Primary care provider refers patient to a hospital-affiliated drug treatment clinic for his addiction under a county program. The addiction center must report treatment information back to the county for program reimbursement, and back to the shelter to verify that the person is in treatment. Someone claiming to be a relation of the homeless man requests information from the homeless shelter on all the health services the man has received. The staff at the homeless shelter is working to connect the homeless man with his relative.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. The extent and amount of information shared between the various facilities would be limited by the minimum necessary guidelines.

18. Health Oversight: Legal Compliance/Government Accountability

Stakeholder organizations and exchanges:

- State university faculty (requesting health information)
- State public health agencies (asked to provide health information)

The governor's office has expressed concern about compliance with immunization and lead screening requirements among low-income children who do not receive consistent health care. The state agencies responsible for public health, child welfare and protective services, Medicaid services, and education are asked to share identifiable patient-level health care data on an ongoing basis to determine if the children are getting the health care they need. This is not part of a legislative mandate. The governor in this state and those in the surrounding states have discussed sharing this information to determine if patients migrate between states for these services. Because of the complexity of the task, the governor has asked each agency to provide these data to faculty at the state university medical campus who will design a system for integrating and analyzing the data. There is no existing contract with the state university for services of this nature.

Potential areas of discussion of BUSINESS PRACTICES based on this scenario:

1. What is the practice of the organization to provide appropriate information for health care oversight activities? These may include:
   - Determining minimum amount necessary.
   - How to release (electronically or paper—with existing claims data).

APPENDIX C
NINE DOMAINS OF PRIVACY AND SECURITY

1. **Authentication:** User and entity authentication to verify that a person or entity seeking access to electronic personal health information is who they claim to be.
2. **Authorization and Access Control:** Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.
3. **Patient and Provider Identification:** Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.
4. **Transmission Security:** Information transmission security or exchange protocols (ie, encryption) for information that is being exchanged over an electronic communications network.
5. **Information Protection:** Information protections so that electronic personal health information cannot be improperly modified.
6. **Information Audits:** Information audits that record and monitor the activity of health information systems.
7. **Administrative Security:** Administrative or physical security safeguards required to implement a comprehensive security platform for health information technology (HIT).
8. **State Law:** State law restrictions about information types and classes and the solutions by which electronic personal health information can be viewed and exchanged.
9. **Policy:** Information use and disclosure policies that arise as health care entities share clinical health information electronically.

APPENDIX D
GLOSSARY OF ACRONYMS

ADD	attention deficit disorder
ADHD	attention-deficit/hyperactivity disorder
AHIMA	American Health Information Management Association
AHRQ	Agency for Healthcare Research and Quality
BAA	business associate agreement
CDC	Centers for Disease Control and Prevention
CLIA	Clinical Laboratory Improvement Amendment
eHIE	electronic health information exchange
EHR	electronic health record
ER	emergency room
FERPA	Family Educational Rights and Privacy Act
FTP	file transfer protocol
HIE	health information exchange
HIPAA	Health Insurance Portability and Accountability Act
HISPC	Health Information Security and Privacy Collaboration
HIT	health information technology
HR	human resources
IAV	Interim Assessment of Variation (of Business Practices, Policies, and State Law)
IHDS	integrated health delivery system
IPWG	Implementation Planning Work Group
IRB	institutional review board
IT	information technology
IVR	Interactive Voice Response
LWG	Legal Work Group
MDR	multidrug resistant
NPI	National Provider Identifier
ONC	Office of the National Coordinator for Health Information Technology
PBM	pharmacy benefit manager
PHI	protected health information
RHIO	regional health information organization
RLS	record locator service
SWG	Solutions Work Group
TAP	Technical Advisory Panel
TB	tuberculosis
TPO	treatment, payment, and health care operations
VPN	virtual private network
VWG	Variations Work Group