

Privacy and Security Solutions for Interoperable Health Information Exchange

Florida's Final Assessment of Variation and Analysis of Solutions Report (Deliverable No. 5)

Subcontract No. 30-321-0209825
RTI Project No. 9825

Prepared by:

Florida Center for Health Information and Policy Analysis
Florida's Agency for Health Care Administration
2727 Mahan Drive, MS. #16 Tallahassee, FL 32308

Submitted to:

Linda Dimitropoulos, Project Director
Privacy and Security Solutions for
Interoperable Health Information Exchange

Research Triangle Institute
P. O. Box 12194
3040 Cornwallis Road
Research Triangle Park, NC 27709-2194

March 30, 2007



Acknowledgements

Florida's Agency for Health Care Administration would like to acknowledge the following members of the Florida Privacy and Security project team for their contributions to this report:

Contributors:

Lisa Rawlins, Project Director and
Bureau Chief, Florida Center for Health Information and Policy Analysis
Agency for Health Care Administration

Carladenise A. Edwards, Ph.D., Project Coordinator
Privacy and Security Project

William Dillon, Health Law Consultant
Privacy and Security Project

Tim Rearick, Information Security Consultant
Privacy and Security Project

Christopher Sullivan, Ph.D., Technical Coordinator
Florida Center for Health Information and Policy Analysis,
Agency for Health Care Administration

Carolyn Turner, Contract Manager
Florida Center for Health Information and Policy Analysis,
Agency for Health Care Administration

Pia Neustadter, Research Analyst
Privacy and Security Project

John Collins, HIPAA Coordinator
HIPAA Privacy and Security Compliance Office
Agency for Health Care Administration

&

Steering Committee, Governor's Health Information Infrastructure Advisory Board

Variations Work Group Members

Legal Work Group Members

Solutions Work Group Members

Table of Contents

Acknowledgements..... i

Executive Summary v

1.0 Background and Purpose..... 2

 1.1 Purpose and Scope of Report..... 2

 1.2 Health Information Technology Development in Florida..... 3

 1.3 Report Limitations 4

2.0 Assessment of Variation Report..... 6

 2.1 Methodology Section..... 6

 2.2 Overview of Scenario Analysis..... 8

 2.3 Treatment (Scenarios 1–4)..... 10

 2.4 Payment (Scenario 5) 21

 2.5 RHIO (Scenario 6)..... 23

 2.6 Research (Scenario 7) 25

 2.7 Law Enforcement (Scenario 8)..... 27

 2.8 Prescription Drug Use/Benefit (Scenarios 9 and 10)..... 30

 2.9 Healthcare Operations/Marketing (Scenarios 11 and 12) 33

 2.10 Public Health/Bioterrorism (Scenario 13) 36

 2.11 Employee Health (Scenario 14) 39

 2.12 Public Health (Scenarios 15–17)..... 41

 2.13 State Government Oversight (Scenario 18) 46

 2.14 Summary of Critical Observations and Key Issues 48

3.0 Summary of Key Findings from the Assessment of Variation 50

 3.1 Variations in Business Practices and Policies..... 50

 3.2 Barriers to Health Information Exchange 50

 3.3 Effective Practices that Protect Privacy and Security..... 51

4.0 Review of Solutions Identification and Selection Process..... 53

 4.1 Methodology Section..... 53

 4.2 Solutions Framework 53

 4.2.1 Legislative Solutions..... 53

 4.2.2 Regulatory Solutions 53

 4.2.3 Organizational / Administrative Solutions 54

4.2.4	Technological Solutions	54
4.2.5	Education and Public Awareness Solutions	54
5.0	Analysis of Proposed Solutions	56
5.1	Legislative Solutions	56
5.2	Regulatory Solutions	58
5.3	Organizational/Administrative Solutions.....	61
5.4	Technology Solutions.....	63
5.5	Education and Public Awareness Solutions	68
6.0	National-Level Recommendations.....	73
7.0	Conclusions and Next Steps.....	76
8.0	Appendices.....	78
8.1	Florida Scenarios	78
8.1.1	FL-1: Medicaid Scenario.....	78
8.1.2	FL-2: RHIO Scenario	80
8.1.3	FL-3: RHIO Scenario	82
8.1.4	FL-4: Personal Health Record Scenario.....	83
8.2	Work Group Members	85
8.2.1	Variations Work Group Members	85
8.2.2	Legal Work Group Members	86
8.2.3	Solutions Work Group Members	87
8.2.4	Steering Committee Members.....	88
8.2.5	HISPC Stakeholder Group Participation.....	89
8.3	Variations Template	93
8.4	Solutions Template	95

EXECUTIVE SUMMARY

Executive Summary

Project Background

Florida's Agency for Health Care Administration (Agency) was awarded a contract by RTI, Inc. to participate in the Health Information Security and Privacy Collaboration (HISPC). This Project is part of a national effort managed by the U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology (ONC), the Agency for Healthcare Research and Quality (AHRQ) and the National Governor's Association (NGA). Florida was one of 34 states and U.S. territories responsible for managing the collection and analysis of data from the state's health care stakeholders on the variations in organizational business practices, policies, and laws related to the private and secure exchange of health information.

The Agency assembled a management team that is knowledgeable about issues related to health information exchange (HIE) and that has experience in the business and legal aspects of health information privacy and security practices. The management team took the lead on organizing core groups of health care stakeholders into work groups that have actively participated in facilitated meetings aimed at collecting data on how policies and laws related to HIE are applied in a number of situations and across a variety of health care environments. The Variations Work Group (VWG) was given the task of reviewing health care exchange scenarios and identifying business practices related to each scenario. This group collected 168 responses to 22 scenarios representing approximately 47¹ different business practices.

The Legal Work Group (LWG) took each of the business practices that had been identified as a barrier to health information exchange and determined the legal challenges related to each barrier. The LWG found that the barriers were a result of inconsistent state and federal laws, misunderstanding or misinterpretation of policies or laws, and the inconsistent application of the policy or law in actual practice. The data collection from these expert focus groups has been used to create a series of reports, including an Interim Assessment of Variation Report (Deliverable 2) and the Interim Analysis of Solutions Report (Deliverable 3). Copies of these reports are available at: http://ahca.myflorida.com/dhit/Privacy_ss.shtml

Purpose of Report

The purpose of the Final Assessment of Variation and Analysis of Solutions Report is to illustrate the variations in organization-level business practices, policies and laws² related to the private and secure exchange of health information. This final report includes an assessment of the variation in business practices, policies and laws and an analysis of the solutions to the barriers caused by the variation. The report contains eight main sections. Section 1 describes the background and purpose of the report. Section 2 is a description of the methodology used to collect and analyze the data presented in this report and a breakdown and analysis of each of the scenarios presented by RTI, including a description of the stakeholders responding to the scenario, the applicable domains, and the general observations of variations in practice and/or law. Section 3 summarizes the key findings from the assessment of variation. Section 4 includes an introduction to the analysis of solutions and describes the process of identifying and selecting solutions. Section 5 is an analysis of the state level solutions and this is followed by a

¹ The estimated 47 is based on the total number of discrete business practices presented in theory, not necessarily on nomenclature.

² The term "law" used here refers to relevant regulation, statute, or case that is the primary underlying driver behind a business practice.

listing of the solutions that serve as national recommendations (Section 6). Section 7 summarizes the entire report and identifies next steps pertaining to the implementation of the proposed solutions. The Appendix (Section 8) includes the analysis of the four Florida scenarios which were added by Florida's Privacy and Security Team and a listing of the work group members.

Notable Observations

There were variations within and across stakeholder groups related to how privacy and security policies were applied to actual business practices as outlined in this report. Some of the variations resulted in barriers to health information exchange, such as inconsistent state and federal laws that resulted in variations in policy, misunderstanding or misinterpretation of policies or laws, and the inconsistent application of the policy or law in actual practice.

A legal barrier to HIE is a statutory or regulatory requirement that prevents the free flow of health information. In order to maintain the confidentiality of personal health information and thereby maintain consumer confidence in the health care system legal barriers to HIE are a necessity. However, many of the laws regulating HIE were created prior to the advent of electronic HIE. Consequently, many such laws are narrowly focused and often prevent or delay, perhaps inadvertently, the free flow of HIE to those who would otherwise be authorized to access the health information. These delays are especially problematic if they prevent timely access to health care, subject people to the stress and hazards of unnecessary tests, and in general, negatively impact people's health and well being.

The solutions outlined in this report address the variations within and across stakeholder groups related to the application of privacy and security policies and laws. Based on the types of barriers identified by the VWG and LWG, the Solutions Work Group (SWG) developed solutions that address laws and regulations to facilitate health information exchange; technical issues related to the secure exchange of electronic health information; administrative or organizational barriers to exchanging health information; and the need for more education and greater public awareness of the rules and laws that address health information exchange.

SECTION 1

Background and Purpose

1.0 Background and Purpose

1.1 Purpose and Scope of Report

Florida's Agency for Health Care Administration (Agency) was awarded a contract by RTI, Inc. to participate in the Privacy and Security Project. This project is part of a national effort managed by the U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology (ONC), the Agency for Healthcare Research and Quality (AHRQ) and the National Governor's Association (NGA). The Agency was one of 34 states and U.S. territories responsible for managing the collection and analysis of data from key health care stakeholders on the variations in organizational business practices, policies, and laws related to the private and secure exchange of health information.

The purpose of the Privacy and Security Project was to conduct a nationwide assessment of privacy and security practices, in partnership with subcontracting States and territories. Its goal is to develop a rational basis for modifying and harmonizing these privacy and security practices in nine domains where variations are known to occur. These are:

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

Variations in privacy and security practices impede information sharing by adding technological and administrative costs to data sharing efforts. The scope of the project has been to identify these variations and to propose solutions to the barriers caused by the variations in privacy and security business practices, policies, and laws. A barrier to health information exchange (HIE) is defined as a business practice or policy that may impede access to health information or health information exchange despite what the law does or does not allow.

For example: A policy that only allows the release of a patient's health information upon the physician's receipt of the patient's written consent regardless of the patient's ability or capacity to complete the required documentation.

Utilizing the experience and expertise of key healthcare stakeholders across the state of Florida, the Agency collected 168 responses to 22 scenarios representing approximately 47³ different business practices. These responses came from numerous stakeholder groups including: clinicians, long term care facilities, physician groups, federal health facilities, hospitals professional associations, payers, public health agencies, community clinics and health centers, consumers, laboratories, state government, pharmacies, and Regional Health Information Organizations (RHIOs). Each response was analyzed by a group of experts who comprised the Variations Work Group (VWG) and another group of experts who served on the Legal Work Group (LWG). The VWG identified the business practices related to each scenario and helped identify instances of variation and barriers to health information exchange. This information was presented to the LWG who conducted a thorough legal analysis of the barriers in preparation for the Solutions Work Group (SWG). The SWG identified a total of 38 solutions that fell into five different categories that represent the identified barriers to health information exchange. The remainder of this report describes the barriers and the solutions as defined by the VWG, LWG, and SWG during the data collection process.

1.2 Health Information Technology Development in Florida

Florida has been a participant in the national movement to improve the quality of health care and health outcomes through the utilization of health information technology since 2004. In the Institutes of Medicines report, *“Crossing the Quality Chasm,”* it is noted that both patients and clinicians can benefit from improvements in care through the use of HIE, specifically through internet-based communication and immediate access to automated clinical information, diagnostic tests, and treatment results. Additionally, researchers have indicated that HIE can enhance equity issues in the health care delivery system by providing a broader array of options for how patients interact with clinicians through increased access to information via the technological infrastructure.⁴

On May 4, 2004, by Executive Order No. 04-93, Florida’s Governor Jeb Bush called for the creation and promotion of a plan for the development and implementation of a Florida Health Information Infrastructure (HII). Former Governor Bush established the Governor’s Health Information Infrastructure Advisory Board to advise the Agency as it develops a strategy and implements the plan. The Governor specifically charged the Board with ensuring that the strategy and plan preserve the privacy and security of health information. Florida’s participation in the Privacy and Security project is one of the ways the Board is working towards this goal.

The Governor’s Health Information Infrastructure Advisory Board was the designated Steering Committee for the Florida Privacy and Security Project. As the Steering Committee for the Florida Project, the Board provided guidance to the Agency’s project management team and oversight in the development of all work products submitted to RTI. In addition to the expertise the Board has brought to the project, the Florida Privacy and Security Project invited the National Conference of Commissioners on Uniform State Laws (NCCUSL) to monitor the state-level discussions and to serve as a resource for the national implementation of privacy and security solutions, including the development of a model state law for electronic health records. The support of the Board and NCCUSL along with the expertise of the stakeholders and

³ The estimated 47 is based on the total number of discrete business practices presented in theory, not necessarily on nomenclature.

⁴ See: National Academy Press. *“Crossing the Quality Chasm: A New Health System for the 21st Century.”* Washington DC. <http://darwin.nap.edu/books/0309072808/html/164.html>.

management team, have contributed to the development of beneficial work products by Florida's Privacy and Security Team.

1.3 Report Limitations

This report combines the key elements of the Interim reports submitted by Florida to RTI. The Florida Privacy and Security Project team has found the interim reports to be useful tools and valuable resources during the development of the Implementation Plans that will be used to address the barriers identified as a part of this project. Some of the challenges faced by the team during the data collection and identification of business practices were:

- Limited amount of time provided to research each scenario
- Concerns from stakeholders over releasing what appeared to be proprietary information when outlining business policies
- Inconsistencies between written policies and actual business practices
- Concerns about the ability to report anonymously
- Distrust of the motives of the federal government
- Limited or lack of use of electronic health information in their health care environment

Despite these challenges to the data collection process, each member of the VWG and LWG was able to solicit business practices related to each scenario and the team was able to produce a variety of solutions and several actionable implementation plans for consideration by the project.

SECTION 2

Assessment of Variation Report

2.0 Assessment of Variation Report

2.1 Methodology Section

The Agency initiated the privacy and security project in June 2006 by assembling a project management team comprised of experts in the field of health information exchange (HIE) and the technical, business and legal aspects of health information privacy and security practices. The management team has taken the lead on organizing core groups of Florida's health care stakeholders and national experts who have actively participated in facilitated meetings aimed at collecting data on how policies and laws related to HIE are applied in a number of situations and across a variety of health care environments.

The data collection began when RTI provided the Agency with a list of 18 scenarios to analyze along nine domains of privacy and security. Each scenario represented a business practice or health care situation that highlighted an exchange or need to exchange health information between different entities. The nine domains reflect issues related to privacy and security and are written in such a way that they are particularly applicable to the exchange or sharing of health information between providers, entities, or across state lines in either a paper or electronic manner. In addition to the 18 scenarios provided by RTI, Florida analyzed four additional scenarios created by the Florida team. The four additional scenarios reflect situations of particular interest to Florida and are included in the appendix of this report.

Florida established four expert panel focus groups to serve as the primary sources of data for the privacy and security project. Each panel or work group had a specific charge related to the completion of the project. The Variations Work Group (VWG) was responsible for analyzing the scenarios and reporting the business practices employed by their respective organizations to address each scenario. The Legal Work Group (LWG) took each of the business practices identified by the VWG members and determined the legal drivers and the legal barriers to health information exchange. These two groups were proceeded by a Solutions Work Group (SWG) and Implementation Planning Work Group (IPWG). The members of these groups helped determine the solutions to the barriers and a plan for implementing the proposed solutions. The following is a brief description of the Variations Work Group and Legal Work Groups role in generating a list of variations and barriers to HIE.

Variations Work Group (VWG). The VWG was formed to identify business practices and policies related to the 18 scenarios provided by RTI and the four additional scenarios provided by the Florida Privacy and Security Team and to determine which business practices were barriers to HIE. Each scenario was evaluated in terms of how it related to the nine domains of privacy and security which were also provided by RTI.

The VWG included 17 members who represented the following stakeholder groups:

- Regional Health Information Organizations (RHIOs)
- Public Health
- Physicians
- Community Health Centers
- Dentists
- Hospitals
- Nurses
- Pharmacists
- Veteran's Affairs
- Managed Care
- Medicaid
- Health Information Management/Academia
- State Government

It also included a representative from the National Conference of Commissioners on Uniform State Laws (NCCUSL). The VWG was chaired by Peter Greaves, a member of the Governor's Health Information Infrastructure Advisory Board (GHIIAB), the project's steering committee.

The VWG met in Tampa, Florida on July 12th and 26th, 2006. During the first meeting, the group was introduced to the scope of the project and to their assigned task. They reviewed the scenarios and domains provided by RTI and identified the business practices and policies related to a few scenarios as examples. By the end of the meeting, the group was able to see how and where variations in business practices existed between stakeholders in response to each scenario. This set the foundation for their assignment and the follow-up meetings where the findings were discussed.

The VWG formed study teams with members of their stakeholder groups to analyze each of the 18 RTI scenarios and the 4 Florida scenarios. The VWG members were asked to have their colleagues review the scenarios, identify business practices and policies and to complete an electronic worksheet that allowed them to document the:

- Business Practice
- Business Policy
- Privacy and Security Domain
- Assumptions made when reviewing the scenario as presented
- Whether or not the practice was a barrier to HIE, particularly in an electronic environment, and
- The Legal Driver or Statutory Reference related to the business policy.

Each stakeholder group was asked to analyze the scenarios and to return their completed worksheets to the Agency in preparation for the Legal Work Group (LWG) meeting. Work group members were provided a template to assist the process (see Appendix 8.3).

Legal Work Group (LWG). The role of the LWG was to identify the legal drivers related to the business practices that were identified as barriers to HIE by the VWG. The LWG was charged with analyzing the business practices presented and forming an opinion as to what laws or regulations apply to the scenario and the stated business practices.

A representative from NCCUSL also participated. The LWG was comprised of 15 attorneys and/or persons who served in a regulatory role for the following stakeholder groups:

- Regional Health Information Organization (RHIO)
- Hospitals
- Public Health
- Dentistry
- Social Welfare and Civil Rights
- Elder Affairs
- Medicaid
- Managed Care
- Private Sector
- Board of Medicine
- Florida Medical Association

The LWG was chaired by Ronald Burns, D.O., a member of the Governor's Health Information Infrastructure Advisory Board.

After receiving their charge from the Project management team in a joint teleconference with the VWG, the LWG held their first face-to-face meeting in Tallahassee, Florida on August 23, 2006. During this meeting the LWG discussed the legal barriers or perceived legal barriers to HIE. Prior to the meeting, members of the LWG received the completed worksheets from the VWG that included the responses to the RTI and Florida specific HIE scenarios. During the meeting the LWG members discussed the stakeholder responses for the following scenarios:

RTI-1:	Patient Care Scenario A (Emergent Transfer of Health Information);
RTI-2:	Patient Care Scenario B (Non-emergent Transfer of Health Information);
RTI-3:	Patient Care Security and Access Scenario;
RTI-4:	Patient Care (Non-emergent Transfer of "Super-confidential" Health Information);
RTI-5:	Payment Scenario;
RTI-6:	RHIO Scenario;
RTI-14:	Employment Information Scenario;
RTI-16:	Public Health Scenario (Newborn Screening);
FL-1:	Medicaid Scenario;
FL-2:	RHIO Scenario.

The legal drivers and federal or state statutory references related to each scenario were discussed in detail during the LWG meeting and further analysis was completed on all of the RTI and Florida scenarios after the meeting. The LWG group members were asked to conduct a detailed legal review of each scenario and to outline the applicable laws, discuss the contradictory laws, and the barriers that the legal drivers may present to ensuring health information was exchanged in a timely, yet secure manner. Upon completion of their review, the LWG analysis was further analyzed by the legal consultant who developed the framework that was used to guide the analysis of variations in business practices that is presented in this report.

2.2 Overview of Scenario Analysis

The collective work of the VWG, the LWG, and their respective stakeholder constituents resulted in the generation of 168 individual responses to the 18 RTI scenarios and the 4 additional Florida scenarios. These responses provided approximately 47 different business practices covering all nine domains. In this section of the report, each scenario is presented with a discussion of the stakeholders who responded to the scenario, the privacy and security domains addressed by the scenario, and the critical observations resulting from the legal analysis.

The 18 scenarios provided by RTI addressed a variety of situations that required the sharing of health information for different purposes, including:

- 4 patient care scenarios
- 1 payment scenario
- 1 RHIO scenario
- 1 scenario related to the use of data for research purposes
- 1 law enforcement scenario
- 2 pharmacy benefit scenarios
- 2 health care operations or marketing related scenarios
- 1 scenario related to bioterrorism
- 1 employment scenario
- 3 public health scenarios
- 1 health oversight scenario

The four additional Florida scenarios expanded upon the issues raised in the RTI scenario to address the use of Medicaid data, 2 additional RHIO scenarios, and a personal health record scenario.

In general, the majority of the business practices generated from the review of each scenario addressed policies related to information use and disclosure between health care entities. The bioterrorism scenario received the most responses and it was the only scenario in which the business practices presented covered eight of the nine domains of privacy and security. The following sections outline the responses to each scenario and highlights the critical findings.

2.3 Treatment (Scenarios 1–4)

RTI provided Florida with four patient care or treatment scenarios. There were 23 responses to the four treatment scenarios and these responses covered six of the privacy and security domains as indicated below.

Treatment Scenarios				
SCENARIOS	RTI-1	RTI-2	RT1-3	RTI-4
DOMAINS				
1. User and Entity Authentication	2		1	1
2. Information authorization and access	1	2	1	4
3. Patient and Provider Identification	1	1	0	1
4. Encryption Protocol			2	
8. State law restrictions		2		1
9. Info use/disclosure	1	4		2
# of Responses	5	9	4	9
# of Domains	4	4	3	5

RTI-1. Patient Care Scenario A

The emergent transfer of health information between two hospitals that represent the 2 stakeholder organizations (i.e. Hospital A and Hospital B) when the status of the patient is unsure. The actors are the staff 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.

General Overview of Stakeholder Business Practice:

There were five responses to this scenario, from a variety of stakeholders including: clinicians, physician groups and hospitals, and a special entry from a long term care facility. The stakeholders considered four domains in their business practices. Clinicians and the long term care facility addressed user and entity authentication (Domain 1); the physician group addressed patient and provider identification across multiple information systems (Domain 3) and the hospital addressed information use and disclosure policies (Domain 9).

The business practices described in this scenario were split between requiring a signed release form from the patient before requesting health care records and not requiring a signed patient consent form based on medical emergency procedures that allow the release of patient health information (PHI) without patient consent. In the first instance, the facility would determine if the daughter had power of attorney to sign for her mother. This appears to be the most common approach, as noted by one respondent: "We see this every day in the ER. We have either the patient or the family member sign a release form and fax it to the hospital holding records on the patient. The hospital usually faxes the information back to us in a timely manner."

In the second instance, the two facilities would contact the out-of-state hospital to obtain records in an emergency situation. However, in both cases where "breaking the glass" was suggested, the respondents noted that the hospital in the other state would need to have similar emergency laws for releasing PHI, or the request for information would not be honored.

In all cases, the difficulty of collecting health care records from an out-of-state hospital was noted. One respondent went so far as to comment that: "If they called a possible hospital that hospital may not even admit that the patient was ever there. If they got the right hospital they would have to find a staff person who would agree to exchange faxes."

Finally, there was a submission from a long term care facility that changed the location of health care service in the scenario to its facility rather than the emergency department. In this special instance, the long term care facility would follow a slightly different business practice to obtain the health care information. Given the confused state of the patient, the facility would first determine if the daughter had power of attorney to sign a consent form for her mother. If the daughter was not a health care surrogate, "then the facility's Admissions Team would assign a temporary health care surrogate in accordance with Florida Statute 755 and admit the resident."

The business practices in summary tend to focus on whether to obtain consent or to use emergency procedures, and whether medical records can be obtained across state lines.

Legal Analysis:

The stakeholders were generally correct in indicating that written authorization was required in order to comply with applicable legal standards. Specifically, the exchange of health information described in the above scenario would implicate both state and federal law.

Florida Law. There are several Florida laws that are relevant when looking at this scenario. §395.3025, F.S., which is applicable to hospitals and ambulatory surgery centers, requires specific, written patient consent in order to perform the health information exchange contemplated in the scenario.⁵ Additionally, the scenario makes reference to medication prescribed to the patient that implies that the patient may have received mental health services. If the patient did receive mental health services from a hospital, §395.3025(2), F.S., would require adherence to §394.4615, F.S., which would call for the “express and informed consent” of the patient or the patient’s guardian prior to release of the information. Fortunately, both patient authorization requirements are substantially similar.

As the patient in the scenario does not appear to be able to provide consent due to her physical incapacity at the time of treatment, the issue of a proxy who is authorized to provide consent also becomes relevant. Under Florida law, §765.205(2), F.S., empowers an appropriately designated individual (health care surrogate) to authorize the release of medical records on behalf of an individual who does not possess the required decision-making capacity.

It should also be noted that this scenario would be treated differently under Florida law if the health information exchange described was requested from a physician’s office in Florida rather than a hospital in Florida. §456.057(7)(a), F.S., allows for the exchange of health information between providers who are involved in the treatment of the patient without requiring the written authorization of the patient.⁶

Finally, while the scenario is silent on whether or not the law enforcement officers investigating the accident are requesting the disclosure of the patient’s health information, it would not be unreasonable to suspect that such a request might be made for accident investigation purposes. Please see the analysis for scenario RTI-8 which specifically raises the issue of disclosure of health information to law enforcement.

Federal Law. As with Florida law there are several Federal laws that would be applicable. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. Interestingly, HIPAA, in general terms, was the most identified legal driver listed by responding stakeholders.

45 CFR §§164.502(a)(1)(ii) and 164.506(c)(2), authorize the use and disclosure of protected health information for treatment, payment and health care operations without the written or oral

⁵ §395.3025(4), F.S., provides that patient consent is required for disclosure absent specific exceptions not applicable to the RTI-1 scenario. §395.3025 (7) (a), F.S., indicates that a general authorization is not sufficient.

⁶ There must be a current treatment relationship in order for a provider to receive patient information under §456.057(7)(a)., See, *Knittel v. Beverly Health and Rehabilitation Services, Inc.*, 863 So.2d 1279, 1281 (Fla. 2d DCA 2004).

consent of the patient. Accordingly, the exchange contemplated in this scenario would be appropriate under the aforementioned regulations.

As almost all hospitals are participants in the Medicare program, 42 CFR §482.13(d)(1), would also be relevant. Under this condition of participation, patients are entitled to a confidential medical record. However, the regulation is silent with regard to requirements for the disclosure of patient information. Interestingly, 42 CFR §431.306(d), which is applicable to the Medicaid program, specifically allows for the emergency disclosure of a recipient's health information. Any such emergency disclosure would require an immediate notification to the recipient or their family after the fact.

Florida Law and HIPAA. While HIPAA would normally preempt a contrary state law, 45 CFR §160.203(b), provides an exception for state laws, such as the ones referenced above, that are more stringent than HIPAA. Consequently, Florida law would be controlling in this scenario. It should also be noted that applicable Medicaid law would also be considered more stringent than HIPAA.

(It should be noted that this scenario contemplated an exchange of information between providers in two different states. Accordingly, the legal analysis above could be different depending on the law of the unnamed state.)

RTI-2. Patient Care Scenario B

The scenario involves the non-emergent transfer of records from a specialty substance treatment provider to a primary care facility for a referral to a specialist. An inpatient specialty substance abuse treatment facility intends to refer client X to a primary care facility for a suspected medical problem. The two 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.

General Overview of Stakeholder Business Practice:

There were nine responses to this scenario from four different stakeholders: clinicians, physician groups, community clinics and health centers, and consumer organizations. Each stakeholder group provided a business practice that addressed a different domain, with clinicians addressing information use and disclosure policies (Domain 9), and physician groups addressing patient and provider identification (Domain 3). The community clinics and health centers presented a business practice that addressed state law restrictions on the information disclosure (Domain 8) and the consumer organizations responded to information authorization and access controls (Domain 2), state law restrictions (Domain 8) and information use and disclosure policies (Domain 9).

The nine responses reflected two different business practices:

- Information disclosed in order to ensure the continuity of care whether patient consent was verified or not. (5 responses)
- Legal documentation required in order to release any patient information. (4 responses)

The clinicians, physician groups and consumer organizations would obtain patient consent before accessing or releasing the patient's substance abuse records and the community clinics and health centers acknowledged disclosure of the patient's records without verification of consent, because it maintained that patient authorization is not required by HIPAA for treatment, payment or health-care operations.

Of interest is that the physician group indicated that its use of patient records was based on the implied consent of the patient. If it received no disclosure of restrictions under 42 C.F.R 2.32 then it had no duty to inquire about any restrictions. "We seek to take all steps relevant to patient care unless prevented by state or federal law. We will not knowingly violate state or federal law to provide care, but we will not knowingly impede care by taking steps to bring legal issues into effect if not required." There was no reference to Florida statutes.

The variation in practice presented by this scenario exemplifies the potential for a barrier to HIE based on the interpretation of state and federal law.

Legal Analysis:

The majority of the stakeholders were aware of the legal requirements under federal law to appropriately disclose health information from a substance abuse treatment facility. The stakeholders were silent as to applicable Florida law.

Florida Law. Generally, §456.057(7)(a), F.S., permits the disclosure of patient information between treating providers without the consent of the patient. However, in the scenario under review, the information to be disclosed is related to the patient's use of drugs and alcohol. §397.501(7)(a), F.S., provides that disclosure of information relating to a patient's substance abuse treatment requires the patient's consent. Florida law does provide exceptions to the consent requirement for medical emergencies, §397.501(7)(a)(1), F.S., and for disclosures to service provider personnel⁷ as needed to perform their duties. The disclosure of patient information in this scenario does not appear to be of an emergent nature nor does it appear to be an exchange between substance abuse service providers.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. The disclosure of health information contemplated in the scenario would not seem to comport with the applicable requirements under HIPAA.⁸ Specifically, §397.501(7)(a), F.S., would require the patient's consent, whereas consent would not be required under HIPAA. Additionally, another applicable federal law has much more stringent requirements. The majority of the stakeholders correctly indicated that 42 CFR Part 2 governs the disclosures contemplated in this scenario.

Specifically, 42 CFR Part 2 provides a very detailed set of requirements governing the disclosure of the health information of a patient that has been or is currently receiving treatment from a federally assisted alcohol or drug abuse treatment program. 42 CFR §2.31 provides the components of an appropriate patient authorization that are very similar to the authorization requirements under HIPAA.⁹ It should also be noted that 42 CFR §2.32 prohibits the re-disclosure of patient information, such as contemplated in the scenario, without the express written consent of the patient. However, 42 CFR §2.51 would permit the disclosure of patient information in the event of a medical emergency.

Florida Law and HIPAA. While HIPAA would normally preempt a contrary state law, 45 CFR §160.203(b), provides an exception for state laws, such as the Florida law referenced above, that are more stringent than HIPAA. Additionally, other applicable Federal law was also found to be more stringent than HIPAA as referenced above.

⁷ The term "service provider", defined under §397.311(28), F.S., would include persons or entities subject licensure under Chapter 397 of the Florida Statutes.

⁸ 45 CFR §164.502 and 45 CFR §164.506 allows for the disclosure of protected health information for treatment, payment and health care operations.

⁹ 45 CFR §164.508.

RTI- 3. Patient Care Scenario C

At 5:30pm 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 login 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.

General Overview of Stakeholder Business Practice:

There were four responses to this scenario covering three different domains. The stakeholder respondents included: hospitals, long term care, community clinics and health centers. Each stakeholder submitted a different business practice, but all of the business practices required the seeker of data to have authorization. The variation existed in the level of verification required and the security of the electronic transmission of information. The hospital respondent mentioned in their business practice a need for data to be transmitted through secure encryption. This does not imply the others did not require this, but the other respondents did not focus on this as a requirement. The community clinics and health centers business practice focused on the need for authorization prior to allowing access to information and the long-term care providers required verification that included receiving some form of identification from the provider and the issuing of a secure password and user id from the facilities IT department. All stakeholder responses had the common theme of security with regard to the information access and information transmission issues raised by the scenario. It is possible the limited variation is due to the limited use of electronic HIE among the stakeholders.

Legal Analysis:

The majority of the responding stakeholders were silent as to the legal drivers that supported their responses.

Florida Law. There are several Florida laws that would potentially be relevant in reviewing the information exchanges discussed in this scenario.

The first health information exchange that must be reviewed is the patient's psychiatrist's attempt to access the patient's hospital discharge summary. Normally, §395.3025(4), F.S., would govern the disclosure of health information from a hospital; however, in this case the scenario indicates that the patient was discharged from a hospital psychiatric unit. Therefore the appropriate authority would be found in §394.4615, F.S.¹⁰ This section of law specifies that either the patient or the patient's guardian provide consent before the patient's record could be disclosed. It should be noted that if the psychiatrist was appropriately credentialed on the staff of the skilled nursing facility, §400.145 (2), F.S., would authorize the psychiatrist to access the patient's records maintained by the nursing facility, including a hospital discharge summary.

Upon completing his examination of the patient the psychiatrist dictated his assessment to an offshore transcription company. The transcribing of the patient record is allowable under Florida law, however, §456.057(11), F.S., would require that psychiatrist have appropriate policies in place to protect the "confidentiality and security" of the medical record. Failure to adequately protect the record could be viewed as a violation of the provider's professional license requirements as provided for in Chapter 456, F.S.

After receiving the transcribed medical assessment, the psychiatrist reviews the medical record and applies his electronic signature to the record.¹¹ The record is downloaded by the psychiatrist's staff into his office record.¹² Finally, an encrypted copy of the patient's medical record is sent via email to the skilled nursing facility. The skilled nursing facility is unable to access the record because they do not have the encryption key. Accordingly, the psychiatrist would need to either provide the encryption key or otherwise take steps to make the patient's record available to the facility.¹³

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. A variety of HIPAA privacy and security regulations would be relevant to the information exchanges discussed in this scenario.

45 CFR §§164.502 and 164.506, would authorize the psychiatrist's accessing of the patient's information for treatment purposes without the patient's consent. Access would need to be viewed in concert with any contrary and more stringent state law, such as mentioned in the section above. Assuming that any consent issues have been resolved, the next relevant issue would be the psychiatrist's ability to access patient information in the skilled nursing facility's electronic medical record.

The skilled nursing facility would be obligated by 45 CFR §164.302, to have certain security standards in place to safeguard electronic patient information. The specific information that the

¹⁰ §395.3025(2), F.S., provides that the requirements of the §394.4615, F.S., are to be followed in situations such as the one presented in this scenario. Interestingly, the results would be substantially the same under both statutes.

¹¹ §668.004, F.S., provides that an electronic signature has the same force and effect as a written signature.

¹² §456.057(11), F.S., would govern the in-office treatment of the patient's information.

¹³ Failure to provide the medical record to the facility in a "legible" manner could be viewed as violation of the psychiatrist's professional license. See, §64B8-9.003, F.A.C.

psychiatrist requested to view was hospital discharge information that had been electronically transferred to the skilled nursing facility. In order for such an exchange to have taken place both the hospital and the skilled nursing facility would need to have in place mechanisms to allow for the secure exchange of health information.¹⁴ In the scenario, the psychiatrist was unable to access the information in the skilled nursing facility's electronic medical record because he did not have a login or password to utilize the system. Although actually delaying patient care, the skilled nursing facility would appear to be compliant with the requirements relating to accessing electronic health information. Specific requirements including, but not limited to, workforce clearance procedures, access authorization, password management and transmission security found in 45 CFR §§164.308, 164.310 and 164.312 would be applicable to the facility.

As mentioned above, the psychiatrist in this scenario upon completing his examination of the patient dictated his assessment via telephone to an offshore transcription company. While this process would be allowed, the psychiatrist, being a covered entity under HIPAA, would be required by 45 CFR §164.502(e) (2), to have a business associate agreement with the transcription company. The business associate agreement would need to meet the requirements found in 45 CFR §164.504(e)(2), and (3). The business associate agreement would, among other things, clearly define the purpose of the exchange of health information between the two parties and require the transcription company to use appropriate safeguards to protect the health information.

Upon the completion of the transcription, the health information was made available to the psychiatrist and his employee via a secure web portal. Similar to the requirements of the skilled nursing facility, the psychiatrist would need to assure that the electronic health information is only accessed by authorized persons and transmitted and maintained in a secure manner. In transmitting the encrypted assessment to the skilled nursing facility, the psychiatrist appears to have followed applicable transmission security requirements found at 45 CFR §164.312.

Florida Law and HIPAA. While HIPAA would normally preempt a contrary state law, 45 CFR §160.203(b), provides an exception for state laws, such as the ones referenced above, that are more stringent than HIPAA. Consequently, Florida law, with regard to the hospital discharge summary, may be more stringent than HIPAA.

¹⁴ The scenario does not indicate the existence of a data sharing or similar agreement between the hospital and the skilled nursing facility, however, such an agreement would be plausible depending on the relationship between the two entities. At a minimum, both the HIPAA privacy and security rules would require that two entities exchange authorized information in a manner that safeguards the information.

RTI- 4. Patient Care Scenario D

The non-emergent transfer of health information. 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.

General Overview of Stakeholder Business Practice:

There were fifteen responses to this scenario from a variety of stakeholders, notably clinicians, long term care facilities and nursing homes, hospitals, public health agencies, and community clinics and health centers. The domains addressed in this scenario included: user and entity authentication (Domain 1), information authorization and access (Domain 2), patient and provider identification (Domain 3), state law restrictions (Domain 8), and information use and disclosure policies (Domain 9). The match between domains and stakeholders shows no clear pattern.

All responses to this scenario agree that the place to start is with patient consent for the release of the patient's records. Each stakeholder would obtain a release of personal health information directly from her. In two of the responses, it was pointed out that two consent forms would be required – one for her imaging records and one for her medical records. Each consent form would be sent to a different location.

One respondent indicated that e-mailing the request form would be sufficient. Five of the eight noted that a fax was sufficient, or US mail. Only one facility expected to rely on a digital transmission over an EHR. Only one stakeholder, hospitals, noted a procedure at State B to check the signature on the consent form to ensure patient identification. All others either assumed an identity check would take place, or did not take it into account.

The responses regarding release of information from the outpatient clinic in State B were somewhat varied. None of the responses indicated that releasing documents across state lines would be a problem. Sending x-ray images was considered a standard data report. However, three of the stakeholders noted that the patient's HIV status could be a problem. They indicated that the clinic in State B might not send any records unless there was a special request, or the clinic would send only the requested PHI and avoid any disclosure of HIV status. Except for the facility assuming digital transmission, all records are sent via US mail.

Only two facilities mentioned the BrCA gene test. One response indicated that it was not an issue "related to non-emergent transfer of health information." The other facility indicated that the patient "can have the BrCa gene test and the results may or may not be easily available. She will not have access to the same test results of her relatives."

In general, all facilities agree on the need for consent by the patient in order to obtain her medical records, though only one stakeholder considered authentication at the clinic in State B. The implications of her HIV status were not consistent, with only half of the respondents recognizing that it could limit the PHI sent to the hospital in State A from the clinic in State B. One stakeholder even noted that the patient "may not have revealed that she has a positive HIV test or that her current illness may be worsening or that she may be in search of a second

opinion.” However, since the scenario stated that complete medical records were requested, an incomplete medical record could create a problem for clinicians in state A.

Legal Analysis:

With the exception of mentioning the adherence to heightened consent requirements, the stakeholders were silent as to applicable legal drivers.

Florida Law. §456.057(7)(a), F.S., would be applicable regarding the release of patient information for treatment purposes from the patient’s outpatient provider and would allow for the release of most patient records without the consent of the patient. §395.3025(4), F.S., would govern the release of the patient’s hospital records and would require the specific consent of the patient.¹⁵ Additionally, the scenario indicates that the patient is HIV positive. Accordingly, any release of medical records would need to comply with the requirements of §381.004, F.S.

§381.004 (3)(e), F.S., governs the release of information related to a patient’s HIV test result and generally requires the patient’s specific authorization.¹⁶ However, the restriction only applies to “HIV test results” which are the laboratory results of the patient reported in the patient’s medical record and do not include HIV test results reported to a medical provider by the patient.¹⁷ The scenario does not provide enough information to determine whether or not information being requested would contain “HIV test results.” It should be noted that that §381.004 (3)(e)(4), F.S., would not require patient consent for an exchange of information (test results) between providers consulting on the patient’s treatment.¹⁸

The scenario also indicates that the patient will be receiving a genetic test for the BrCa gene. Under §760.40(2)(a), F.S., the test results become the exclusive property of the patient and may only be released with the consent of the patient.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. 45 CFR §164.502(a)(1)(ii) and 164.506(c)(2) authorize the use and disclosure of protected health information for treatment, payment and health care operations without the written or oral consent of the patient. 45 CFR §164.312(e) would also be applicable in the event that the digital images, or any other electronic protected health information, were to be transmitted electronically.

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would seem to be more stringent than HIPAA.

¹⁵ See also §59A-3.270(7), F.A.C., which limits disclosure of patient information without the patient’s consent to hospital personnel.

¹⁶ See also §64D-2.003(b), F.A.C.

¹⁷ §381.004(2)(b), F.S.

¹⁸ The Florida Department of Health publishes a guide, *Florida’s Omnibus AIDS Act - A Brief Legal Guide for Health Care Professionals*, that is very instructive on the use and disclosures of HIV information under Florida law.

2.4 Payment (Scenario 5)

RTI- 5. Payment Scenario

Health Payer (third party, disability insurance, employee assistance programs) provides health insurance coverage to many subscribers in the region the healthcare 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 (e.g., emergency department records, clinic notes, etc.).

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 healthcare provider's workforce members and medical staff members and their office staff.

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

General Overview of Stakeholder Business Practice:

RTI Provided the Agency with one payment scenario. The VWG received five responses within three of the privacy and security domains: Information authorization and access (Domain 2), State law restrictions (Domain 8), and information use and disclosure (Domain 9). The responding stakeholders (long-term care and payors) generally confirmed that the practice referenced in the scenario is a routine exchange of information between covered entities. The three discrete business practices described included:

- The sharing of information with other entities with the proper information use and disclosure policies in place
- The need for patient consent to be obtained by payer prior to any disclosure
- In the absence of an electronic health record system adherence to state law restrictions on disclosing patient information.

Legal Analysis:

The stakeholders identified patient consent as the primary legal driver in this scenario. One stakeholder indicated that patient consent was not necessary as the exchange was authorized under HIPAA. The stakeholders did not address issues related to accessing the provider's electronic health record.

Florida Law. §456.057(7)(a), F.S., would require that there be patient consent for the provider to disclose the patient's information to the health payer in this scenario. §395.3025, F.S., would be applicable in the case of disclosure from a hospital to a health payer. The disclosure of patient information related to certain conditions could also create the need for specific patient authorization as opposed to general consent.¹⁹ In addition to patient authorization, §456.057 (11), F.S., would require the health care provider to have policies and procedures in place to

¹⁹ For example: §381.004(3)(e)(2), F.S., (HIV Test Results); §394.4615, F.S., (Mental Health Records); §397.501(7), F.S., (Substance Abuse Records) and §760.40, F.S., (Genetic Testing).

protect the confidentiality and security of patient information. Any authorized access to the provider's EHR would need to be addressed in the appropriate policies and procedures. §456.057 (12), F.S., would require that the health provider maintain a record of all patient information disclosures to third parties such as the health payer in this scenario.

A health payer, upon receiving access to the patient information would be required to maintain the confidentiality of such information. Although addressed in several different chapters of the Florida Statutes, it is clear that health insurers, like health providers, are obligated to protect patient information.²⁰ Finally, it should also be noted that employers who provide or administer health insurance benefits may also be subject to certain confidentiality requirements.²¹

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. 45 C.F.R. §§164.502(a)(1)(ii) and 164.506(c)(3) authorize the use and disclosure of protected health information for payment purposes without the written or oral consent of the patient. Accordingly, the exchange contemplated in this scenario would be appropriate under the aforementioned regulations.

Assuming that patient consent had been obtained, the disclosure of the patient's health information should be limited to the minimum necessary for health care payer to complete their treatment review.²² The provider allowing payer access to his electronic health record would be required to adhere to the security requirements found in 45 CFR §§164.306, 164.308, 164.310 and 164.312.

Finally, as a covered entity the health payer upon receiving the information could only use or disclose the patient information as allow under HIPAA.

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would seem to be controlling.

²⁰ For example: §636.064, F.S.,(Prepaid Limited Health Service Organizations); §624.91(8), F.S., (relating to records maintained by the Florida Healthy Kids Corporation); §641.54(5)(c), F.S., (requiring HMO's to provide subscribers with information relating to the organization's patient records policies and procedures); §627.4195, F.S., (Health Insurers and information related to psychotherapeutic services, see also, §641.59, F.S., (HMO records of psychotherapeutic services)).

²¹ §760.50(5), F.S., (Discrimination of the basis of AIDS, AIDS-related complex, and HIV prohibited) which requires employers to maintain the confidentiality of information relating to persons covered by insurance benefits provided or administered by the employer.

²² See 45 CFR 164.502(b)(1).

2.5 RHIO (Scenario 6)

RTI- 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.

General Overview of Stakeholder Business Practice:

The RHIO scenario presented by RTI received four responses. Three addressed the domain related to information use and disclosure (Domain 9) and one of the business practices identified the state law restrictions applied to the release of Medicaid information (Domain 8). The responding stakeholders, including three RHIO respondents and one payor organization, indicated that information exchange in the above scenario would be allowed if authorized by law or if the requested information were de-identified. It should be noted that the scenario reviewed by the stakeholders did not specifically indicate that the data to be disclosed would be identifiable patient data. The RHIO respondent assumed that if the Medicaid State Plan authorized the release of information then the data would be accessible for the purposes of auditing.

Legal Drivers:

The stakeholders provided little information regarding the applicable legal drivers other than to reference the applicability of HIPAA.

Florida Law. The ability to disclose identifiable patient data to a RHIO as described in the above scenario is contingent on the RHIO's structure, in some respects. Specifically, there may be a difference in outcome if the RHIO were operated by the State of Florida, as opposed to a private entity.

In the context of a RHIO operated by a private entity, both §456.057(7) (a), F.S., and §395.3025(4), F.S., arguably require the consent of the patient before the providers participating in the RHIO would be able to release identifiable patient information to the RHIO. If the disclosure of information described in the scenario was within the scope of the consent signed by the patient, then the release of health information would be appropriate.

Although the aforementioned statutes require patient consent to disclose identifiable patient information in certain circumstances, neither statute provides clear guidance as to the disclosure of patient information to a RHIO in which the hospital or the health care provider is a participant.²³ Depending on the role of the RHIO in aiding its participants in the performance of their health care operations patient consent may not be required.

If the RHIO were operated by the State of Florida, the state RHIO could, in all likelihood, have the appropriate statutory authority to access identifiable patient data from participating providers. For example, §408.05, F.S., authorizes the Florida Agency for Health Care

²³ It should be noted that the Florida Statutes do not at this time clearly address the concept of electronic health information exchange nor do they address the concept and function of a RHIO type organization.

Administration via the Florida Center for Health Information and Policy Analysis to collect patient data similar to the data requested in the scenario. Such data would be treated as confidential data under §408.061 (7), F.S.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. 45 CFR §§164.502 and 164.506, generally permit a covered entity to disclose protected health information for treatment, payment or health care operations. The requested disclosure from the participating providers in the RHIO could possibly be considered to fall under health care operations which is defined in 45 CFR §164.501. Specifically, if the RHIO, in accord with business associate agreements²⁴ between it and the providers, were collecting the data for a purpose such as outcomes evaluation and development of clinical guidelines the disclosure would arguably be allowed without the need for patient consent.

In the event that disclosure of identifiable patient data contemplated in the scenario were not considered to be health care operations, a patient authorization compliant with 45 CFR §164.508 would be required.

It should be noted that the disclosure of patient information to the RHIO would not require patient authorization in the event that patient information were de-identified as specified under 45 CFR §164.514. It would also be acceptable to provide the RHIO a limited data set²⁵ provided that the providers and the RHIO had entered into a data use agreement as required by 45 CFR §164.514(e)(4).

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would seem to be controlling.

²⁴ 45 CFR. §164.504(e).

²⁵ 45 CFR §164.514(e)(2).

2.6 Research (Scenario 7)

RTI- 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 is all electronic and all responses from the subjects are completed electronically on the same centralized and shared data base file.

The principle 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 six months and/or use the raw data collected for a white paper that is not part of the research protocols final document for his post doctoral fellow program.

General Overview of Stakeholder Business Practice:

The one research data use scenario received three responses resulting in the description of one business practice that covered three different domains, including:

- Information authorization and access (Domain 2)
- State law restrictions (Domain 8)
- Information use and disclosure (Domain 9)

Both the state government representative and the academic respondent agreed that they would not release the requested data if the release was not consistent with the original data release agreement. Additionally, the academic stakeholder indicated the requestor would need to submit such request after obtaining appropriate Institutional Review Board (IRB) approval and HIPAA waivers of authorization. There was no variation in the responses to this scenario and little speculation on how it would vary in an electronic environment.

Legal Drivers:

The stakeholder cited HIPAA and §408.061, F.S., as the applicable legal drivers.

Florida Law. §408.061(10), F.S., authorizes the Agency for Health Care Administration, which includes the Florida Center for Health Information and Policy Analysis, to serve as the primary source for the collection and dissemination of health care data for the State of Florida. In the event that the information to be used for the extended tracking and the white paper had been obtained from the Florida Center for Health Information and Policy Analysis, such use would be subject to the requirements of a data use agreement between the parties. The data use agreement, among other things, would address the permissible uses and disclosures of the data. If the use of the data as contemplated in the scenario was not consistent with the data use agreement, such use would not be allowed.

Additionally, §405.01, F.S., should also be mentioned as it provides for the disclosure of patient information relating to the patient's condition and treatment to certain study groups²⁶ for the purposes of reducing morbidity or mortality. If the use of the information as contemplated in the scenario were deemed to comply with §405.01, F.S., it would seem to be a lawful disclosure under Florida law. Pursuant to §405.03, F.S., the identity of any person whose condition or treatment has been studied shall be confidential. However, it does not appear that §405.01, F.S., is more stringent than HIPAA and would be preempted.

Federal Law. Research activities such as the ones contemplated in the scenario are normally subject to regulation under 45 CFR Part 46 (the Common Rule) and/or 21 CFR Part 50 (applying to clinical investigations regulated by the Food and Drug Administration). Additionally, 45 CFR Part 164 would also be applicable to the use of information contemplated in this scenario.

Both 45 CFR §46.116(5) and 21 CFR §50.25(5), require that the research subject be provided with informed consent as to the extent, if any, that the confidentiality of the records identifying the subject will be maintained. However, such informed consent is primarily related to the individual's participation in the study. In order to use or disclose such information an authorization that is compliant with 45 CFR 164.508 would be required.²⁷

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164, are also applicable to the health information exchange contemplated in this scenario. Subject to an applicable exception, a new authorization would need to be obtained for any additional uses of information not mentioned in the individual's authorization.²⁸ 45 CFR §164.512(i)(1)(i), provides that a covered entity may use or disclose protected health information for research provided that an appropriate alteration or waiver of the individual's authorization is obtained.²⁹

Finally, 45 CFR § 164.514(e)(3), would allow the covered entity to disclose a limited data set³⁰ for the purposes contemplated in the scenario. Prior to releasing the limited data set the parties would need to enter into a data use agreement as required by 45 CFR §164.514(e) (4).

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would seem to be consistent with HIPAA with the exception of §405.01, F.S., which would be preempted by HIPAA.

²⁶ Specifically indicated in the statute are; research groups, governmental health agencies, medical associations and societies and in-hospital medical staff.

²⁷ See http://privacyruleandresearch.nih.gov/clin_research.asp, *Clinical Research and the HIPAA Privacy Rule*, National Institutes of Health, posted February 5, 2004.

²⁸ See 45 CFR §164.508(c)(iv), requiring a description of each purpose of the requested use or disclosure.

²⁹ 45 CFR §164.512(i)(1)(i)(A-B) provides that an Institutional Review Board or Privacy Board may approve an alteration or waiver of an individual's authorization. Any alteration or waiver would be subject to the requirements of 45 CFR §164.152(i)(2)(ii -iii).

³⁰ 45 CFR §164.512(e)(2).

2.7 Law Enforcement (Scenario 8)

RTI - 8. Scenario for access by law enforcement

An injured nineteen (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 their parent's health and auto insurance policy.

General Overview of Stakeholder Business Practice:

The law enforcement scenario was a common situation to most of the stakeholders. It was discussed in both VWG meetings and during the LWG meeting. Six written responses were collected covering three domains: information authorization and access (Domain 2), information audits (Domain 6), and state law restrictions (Domain 8). Despite the variation in stakeholder respondents, clinician, physician, hospital, and community clinic, there was very little variation in the reported business practices for this scenario and in the applicable laws at the state and federal level.

In this scenario the stakeholders identified two separate health information disclosure issues. First, the stakeholders identified the issue related to the disclosure of health information to law enforcement. Virtually all of the stakeholders indicated that law enforcement would not have access to the patient's blood alcohol and drug screens. (It should be noted that the original scenario reviewed by the responding stakeholders did not specifically indicate that the police were investigating a traffic accident). Second, the stakeholders identified the issue relating to the request by the patient's parents for the disclosure of health information concerning their adult child. As with the disclosure to law enforcement, the stakeholders indicated that the patient's parents would not have access to their adult child's information without the child's consent or authorization. Lastly, one stakeholder indicated that if any information was disclosed that this needed to be documented and available for auditing purposes.

Legal Drivers:

The identification of legal drivers by the stakeholders was, on the whole, sparse and generalized. On the issue of disclosure to the adult patient's parents, the stakeholders correctly indicated that such disclosure would be inappropriate. As for their responses regarding the disclosure to law enforcement, the stakeholders applied practices that would comply with Florida law. However, it should be noted that the result in the above scenario might be different in the event that law enforcement requested the performance of the drug and alcohol screens.

Florida Law.

Release of Information to Law Enforcement

In this scenario, blood alcohol and drug screens were done by the hospital as part of the hospital's routine medical treatment. Law enforcement requested the results of the hospital. Under §395.3025(4), F.S., the patient must consent to the release of such information. In the event that the patient refused to consent to the release of the test results, the results could be obtained via §395.3025(4) (d), F.S., which provides that a hospital may release a patient's information without the patient's consent in response to a valid civil or criminal subpoena provided that proper notice has been provided to the patient.³¹ It should be noted that this scenario might be different in the event that law enforcement had requested the drug and alcohol screen.

§316.1932(1)(c), F.S., provides that any person who holds a Florida driver's license has been deemed to have given consent for a blood test to determine the alcohol content of their blood or to determine the presence of a controlled substance in their blood. In the event that the person presents to an emergency room or other medical facility, a law enforcement officer may request that the person's blood be tested if there is reasonable cause to believe the person was driving under the influence. The individual would be provided with the opportunity to refuse the request of the law enforcement officer.³² In the event that person is incapacitated or otherwise incapable of giving consent the person will be deemed to have given consent. If the test is conducted pursuant to the request of law enforcement, §316.1932(3), F.S., provides that "information relating to the alcoholic content of the blood or breath or the presence of chemical substances or controlled substances in the blood obtained pursuant to this section shall be released to a court, prosecuting attorney, defense attorney, or law enforcement officer in connection with an alleged violation of s. 316.193 upon request for such information". Finally, §316.1932(1)(f)(2) (b), F.S., provides that a health care provider that is providing medical care to an individual that has been involved in a motor vehicle accident "may" notify law enforcement of blood alcohol results in excess of the amount allowed by law.

Release of Information to Parents

In the scenario the parents of the patient requested to see information in the patient's medical record related to the results of a drug screen on the patient. Although the patient is an adult, the patient is on the parents automobile and health insurance policies.

As with the request from law enforcement mentioned above, §395.3025(4), F.S., would prevent the parents from reviewing their adult child's hospital records without his consent.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. With regard to the potential disclosures to law enforcement 45 CFR §164.512(e) would authorize disclosure of the patient's information pursuant to a subpoena or other lawful process. Such procedure would be substantially consistent with the requirements found in §395.3025(4), F.S. Additionally, 45 CFR §164.512(a), which allows the disclosure of protected health information "as required by law" would be applicable to provide the patient's screening results to law enforcement in situations in

³¹ See, *State of Florida v. Johnson*, 814 So.2d 390, (Fla. 2002), in which the Florida Supreme Court discusses the balancing of a patient's right to privacy under the Florida Constitution against the government's legitimate need to access a patient's medical records.

³² It should be noted that while not applicable to the RTI-8 scenario, §316.1933, F.S., would authorize the forceful taking a blood sample in cases in which there was an accident that resulted in death or serious bodily injury.

which law enforcement initiated the blood test. Both of the aforementioned disclosures would be subject to the “minimum necessary” standard found at 45 CFR §164.502(b).

The request by the parents of the adult patient would not be authorized under HIPAA and would require the authorization of the patient pursuant to 45 CFR §164.508. As the policy holders of both the adult patient’s auto and health insurance, the patient’s parents would likely receive an explanation of benefits (EOB) indicating the performance of the tests. The EOB would not normally contain the actual results. However, under 45 CFR §164.522 (b)(1) (ii) the individual could request that the health plan provide the EOB in a confidential manner if the individual felt that the disclosure would place the individual in danger.

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would seem to be consistent with HIPAA. With regard to the disclosure to law enforcement, the crucial legal driver would be what is actually required by Florida law.

2.8 Prescription Drug Use/Benefit (Scenarios 9 and 10)

RTI- 9. Pharmacy Benefit Scenario - A

The Pharmacy Benefit Manager (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.

General Overview of Stakeholder Business Practice:

RTI presented Florida with two pharmacy benefit scenarios, RTI -9 and RTI- 10. There were two responses received to RTI-9 and no responses to RTI-10. The business practice presented addressed information transmission security (Domain 4) and the information use and disclosure domain (Domain 9) and it was presented by a clinician. The responding stakeholder indicated that patient authorization would be needed prior to the physician disclosing any information and that in the absence of a secure electronic encryption method that the data would be transmitted via telephone or fax machine. There were not enough responses to identify variation or any barriers to HIE in this scenario.

Legal Drivers:

The stakeholder provided no legal driver addressing the exchange of information.

Florida Law. §456.057(7)(a), F.S., would authorize a physician to disclose a patient's information to a health care practitioner or provider, without the patient's consent, for the care or treatment of the individual. The term "health care practitioner" is defined in §456.001(4), F.S., and would not include the PBM. The term "provider" is not defined. If the PBM were to be considered a "provider" and the exchange of information was deemed to be for the care of the patient, in this case coordination care may be applicable, no patient authorization would be necessary. §465.0156, F.S., provides the criteria for an out of state pharmacy, "nonresident pharmacy", such as described in the scenario, to provide pharmacy services via mail or other mode of delivery in the State of Florida. As an entity required to be registered with the State of Florida, the mail order pharmacy could arguably be considered to be a provider of health services.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. If the PBM, via its operation of a mail order pharmacy, is considered a covered entity under HIPAA³³ the exchange of information contemplated in the scenario, arguably for coordination of care, would not require the patient's consent.³⁴ Additionally, the self-insured employer, a hospital, is a covered entity both as a health care provider and in its status as a health plan.³⁵ The PBM, in its role as a

³³ 45 CFR §160.103.

³⁴ 45 CFR §164.506(c)(2).

³⁵ 45 CFR §160.103.

benefits manager, would likely be a business associate of the hospital.³⁶ The physician would be able to communicate with the PBM in its capacity as a business associate of hospital's health plan.³⁷ Finally, any protected health information exchanged electronically would need to comply with the requirements of 45 CFR §§164.306, 164.308, 164.310 and 164.312.

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would seem to be consistent with HIPAA if the PBM, via its status as a mail order pharmacy provider, was considered a provider under §456.057(7)(a), F.S.

RTI- 10. Pharmacy Benefit Scenario - B

A Pharmacy Benefit Manager 1 (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 the 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.

General Overview of Stakeholder Business Practice:

The were no stakeholder responses to this scenario

Legal Drivers:

N/A

Florida Law:

As a self-insured plan, Company A would be regulated by the applicable provisions of the Employee Retirement Income Security Act of 1974 (ERISA).³⁸ As an ERISA covered plan, Florida insurance law would be preempted by the more expansive federal law. However, Florida law may, indirectly, impact the proposed scenario. For example, Florida law prohibits the redisclosure of medical records received by a third party without the expressed written consent of the patient or the patient's representative.³⁹ Therefore if the claims data referenced in the scenario were to be considered part of the patient's medical record, which is arguable, patient consent may be required.⁴⁰ It should be noted that PBM could be considered as an "agent" of the self-insured plan and therefore the any disclosure of medical records to the PBM

³⁶ Id.

³⁷ See, <http://healthprivacy.answers.hhs.gov>, HHS Office of Civil Rights, Frequently Asked Questions, Answer ID# 241, providing that a covered entity may provide protected health information to the business associate of another covered entity.

³⁸ 29 U.S.C. §1144(a), provides that ERISA supersedes any state law that would related to an employee benefit such as an employer self-insured plan.

³⁹ See 456.057(12), F.S., applicable to records released by health care practitioners and 395.3025(7) applicable to records released by hospitals.

⁴⁰ 456.057(6), F.S., seems to indicate that "insurance information" which relates to the treatment of an individual is among the information that would be considered part of the medical record.

would not be considered a redisclosure under Florida law. Regrettably, Florida law is not clear on this matter.

Florida law does not directly regulate the operation and/or licensing of pharmacy benefit managers or “PBMs”.⁴¹ However, PBMs could be subject to regulation under Florida law indirectly. For example, as referenced in the previous scenario (RTI-9), a PBM that operates a mail order pharmacy would be obligated to comply with applicable Florida laws relating to pharmacy licensing and operations.

Federal Law:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. Company A’s self-insured plan would in all likelihood be considered a health plan as defined under 45 CFR §160.103. It would also be considered a covered entity under the same section. As a covered entity, Company A would be authorized to utilize protected health information, without the consent of the individual, for treatment, payment or health care operations.⁴² As contemplated in the scenario, the release of information to PBM1 would be considered health care operations⁴³ as the disclosure would be for activities relating to the creation of a contract for health benefits. However, Company A would need to enter into a business associate agreement pursuant to 45 CFR §164.502(e)(2) and 45 CFR §164.314, prior to the disclosure of the information. Additionally, Company A would need to comply with the minimum necessary standard in releasing claims information to PBM1.⁴⁴

Any electronic health information to be exchanged would need to be exchanged in a manner that would be compliant with 45 CFR §§164.306, 164.308, 164.310 and 164.312.

Florida Law and HIPAA:

HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law may conflict with HIPAA in the event that information to be disclosed to the PBM was considered to be a third party redisclosure of information.

⁴¹ See Florida Office of Program Policy Analysis & Government Accountability Report No. 07-08, *Legislature Could Consider Options to Address Pharmacy Benefit Manager Business Practices*, February 2007.

⁴² 45 CFR §164.502(a)(1)(ii) and 45 CFR §164.506(c)(1).

⁴³ 45 CFR §164.501, Health Care Operations (3).

⁴⁴ 45 CFR 164.502(b) and 45 CFR 164.514(d).

2.9 Healthcare Operations/Marketing (Scenarios 11 and 12)

There were four responses to the two healthcare operations and marketing scenarios. There were only two distinct business practices and they fell in the area of information authorization and access and information use and disclosure.

RTI-11. Health Care Operations and Marketing – Scenario A

ABC Health Care is an integrated health delivery system comprised 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.

General Overview of Stakeholder Business Practice:

This scenario received three responses from two unidentified stakeholder groups. The responding stakeholders identified patient marketing and analysis of hospital system data as the relevant issue in the scenario. The business practices of the stakeholders centered on obtaining patient authorization prior to marketing and utilizing abstracted data for analysis. The business practices described addressed information authorization and access (Domain 2) and information use and disclosure (Domain 9). One of the respondents explicitly indicated that the use and disclosure of personal health information for marketing purposes was prohibited, while the other respondent stated that patient information could be disclosed with the patient's written consent.

Legal Drivers:

The stakeholders identified Florida law regarding patient authorization as the applicable legal driver.

Florida Law. Both §395.3025(7)(b), F.S., regarding hospitals and §456.057(7)(b), F.S., regarding health care providers, prohibit patient marketing activities absent a specific written

authorization. Under this scenario patient authorization would be required prior to any marketing activities.

The requirements for the use of patient encounter data to analyze trends within the integrated delivery system would be dependent on the actual structure of the integrated delivery system. If the integrated delivery system in this scenario has a common owner, patient authorization would not be required for the system to analyze its own data.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. Although not enough information was provided to be certain, it appears that the integrated delivery system in this scenario would be considered as an “organized health care arrangement” under 45 C.F.R. §160.103. If the system is considered to be an organized health care arrangement, 45 C.F.R. §164.506(c) (5), would permit the exchange of identifiable patient data contemplated in the scenario without the patient’s authorization for the purposes of health care operations. However, 45 C.F.R. §164.508(a)(3), would, similar to Florida law, require the patient’s authorization to allow the system to use their patient information for marketing purposes.

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would not seem to conflict with HIPAA with regard to the treatment of marketing. Florida law may conflict with the health care operations disclosures depending on the corporate structure of the integrated delivery system.

RTI – 12. Healthcare Operations and Marketing - Scenario B

ABC hospital has approximately 3,600 births/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. They will sell the data to a local diaper company to use in marketing diaper services directly to parents.

General Overview of Stakeholder Business Practice:

The stakeholder responding to this scenario indicated that the acceptable business practice would be to obtain patient consent prior to any of the marketing contemplated in the scenario. The domain addressed was information authorization and access controls.

Legal Drivers:

While applying an appropriate business practice the responding stakeholder did not identify any applicable legal drivers to support the practice.

Florida Law. §395.3025(7)(b), F.S., would prohibit the use of patient information for marketing activities. Accordingly, the uses contemplated in the scenario would require the patient's written authorization.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. Generally, 45 CFR §164.508(a)(3), would require a covered entity to obtain the patient's written authorization in order to conduct marketing activities. Exceptions to the authorization requirement would be face to face communications from the covered entity to the individual⁴⁵ or a promotional gift of nominal values provided by the covered entity.⁴⁶

However, communications that are for the treatment or care coordination of the individual would not be considered marketing under HIPAA.⁴⁷ Therefore, it could be argued that the communications for the first two purposes described above would not be considered marketing and would not require patient authorization.⁴⁸ The remaining two purposes would be considered marketing and require the patient's authorization. Further, if the marketing involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.⁴⁹

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law, §395.3025(7)(b), F.S., would preempt the less restrictive provisions of HIPAA.

⁴⁵ 45 CFR §164.508(a)(3)(i)(A).

⁴⁶ 45 CFR § 164.508 (a)(3 (i)(B).

⁴⁷ 45 CFR §164.501, Definitions - Marketing (1)(ii) & (iii).

⁴⁸ 45 CFR §164.506(b)(1).

⁴⁹ 45 CFR § 164.508(a)(3)(i)(B)(ii).

2.10 Public Health/Bioterrorism (Scenario 13)

By far this was the most popular scenario of the 22 scenarios presented to the VWG and their constituents. Fifty-seven responses were received from six stakeholder groups addressing eight of the nine domains of privacy and security as indicated below:

BIOTERRORISM	
SCENARIO	RTI-13
DOMAINS	
1. User and Entity Authentication	7
2. Information authorization and access	6
4. Encryption Protocol	11
5. Protections from modification	6
6. Information audits	6

BIOTERRORISM	
SCENARIO	RTI-13
DOMAINS	
7. Physical Environmental Protections	6
8. State law restrictions	6
9. Info use/disclosure	9
# of Responses	57
# of Domains	8

RTI- 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 informing the regional media to alert the public to symptoms and seek treatment if feel 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 they arise to identify the source of the anthrax, locate and prosecute the parties responsible for distributing the anthrax, and protect the public from further infection.

General Overview of Stakeholder Business Practice:

This scenario produced the highest number of stakeholder responses. The business practices indicated by the responding stakeholders varied; however, all addressed protecting the confidentiality of patient information. The responses came from clinicians, physician groups, federal health facilities, hospitals, public health agencies, community clinics and health centers, and laboratories. The different business practices presented for this scenario included:

- Adherence to state laws on the exchange of health information in the event of an emergency (19 responses)
- Ensuring state reporting requirements are met and that procedures are in compliance with HIPAA's use and disclosure policies (3 responses)
- Requiring entity authentication prior to the release of health information (6 responses)
- The establishment of data integrity processes, policies, and procedures within and between the entities sharing information (6 responses)
- Limiting access to personal health information to authorized personnel within the department of health (5 responses)
- Verifying the identity of the data recipient prior to releasing the information (1 response)
- The use of technology to authenticate users and to control access (5 responses)
- The establishment of secure data transmission processes between entities that share the information (6 responses)
- Establishment of an events transaction log that time stamps access and receipt of information to create an audit trail (6 responses)

The variability occurred in the extent to which the respondent depended on state law versus HIPAA, the requirements for verification and/or authorization of data exchangers, and the establishment of processes to verify the integrity of the data and to track the release of information in an automated fashion. This scenario presented clear differences in practices based upon the use of a paper versus an electronic system. The utilization of an electronic system provided more controls as opposed to the paper system that depended on telephone and faxes, which do not allow for extensive verification, authentication, and auditing needed in the event of an emergency.

Legal Drivers:

The stakeholders identified numerous legal drivers to support their business practices. However, there was no consistency among the stakeholders with regard to the specific legal drivers identified.

Florida Law. There are several sections of Florida law that are relevant to this scenario. §381.0031(1), F.S., requires that medical providers and licensed laboratories report to the Florida Department of Health any diseases of public health significance. (It should be noted that county health departments are units of the Florida Department of Health). §64D-3.002(1) (c), F.A.C., defines anthrax as a disease or condition of public health significance.⁵⁰ Accordingly, the notification by the laboratory to the health department would be appropriate. §64D-3.003, F.A.C., would require the reporting laboratory to provide certain information identifying the test subject, including locator information.

As the event was determined to be a bioterrorism event an emergency situation was declared. In such case §943.03101, F.S., authorizes the Florida Department of Law Enforcement to oversee and coordinate the response in accordance with the State of Florida's comprehensive emergency management plan.⁵¹ Notification to the media, providing limited information, would

⁵⁰ Diseases of public health significance are, pursuant to §64D-3.002(2), F.A.C., normally required to be reported within 72 hours of discovery. However, in the case of anthrax and certain other specified conditions immediate telephone notification to the Department of Health is required.

⁵¹ §252.35(2)(a), F.S.

be appropriate under §381.00315(1)(b), F.S., which addresses the declaration of a public health emergency.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. 45 CFR §164.512(a) would authorize the disclosure of patient information if required by law and 45 CFR §164.512(b) would authorize the disclosure of the patient information for public health purposes.

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would not conflict with HIPAA.

2.11 Employee Health (Scenario 14)

RTI-14. Patient Care Scenario A

An employee (of any company) presents in the local emergency department for treatment of a chronic condition that has exacerbated which is not work-related. The employee's condition necessitates a four-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 email to the Human Resources department of the patient's employer.

General Overview of Stakeholder Business Practice:

RTI presented one scenario that addressed issues related to exchanging information between providers and employers. The five business practices presented addressed three different domains, including:

- Information authorization and access (Domain 2)
- Information transmission security (Domain 4)
- Information use and disclosure (Domain 9)

The responding stakeholders, including clinicians and public health agencies, indicated that the situation described in this scenario would be dependent on the patient providing authorization to release the information; however, in general the information use and disclosure policies cited did not authorize the release of information to the employer. The one stakeholder that did indicate that information would be shared, required multiple authentication and verification prior to sharing the information and the release of the information through a secure encryption protocol.

Legal Drivers:

Most of the stakeholders indicated the applicable Florida law as the appropriate legal driver for their business practice.

Florida Law. §395.3025(4), F.S., would require the written authorization of the patient to release the information in the manner contemplated by the scenario. Similarly, §456.057(7)(a), F.S., would impose the same authorization requirements for a request made in an office practice setting.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. 45 CFR §164.508, would require that the employee in the above scenario provide a written authorization for the information exchange contemplated. 45 CFR §164.502(b), would require the sender of the information to comply with minimum necessary standard unless the employee authorized a

broader disclosure. Finally, 45 CFR §164.312, would be applicable to the electronic transmission of the information.⁵²

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would not conflict with HIPAA.

⁵² 45 CFR §164.312(e)(2)(i & ii), would specifically address the integrity controls and encryption standards for information transmitted over an electronic communications network.

2.12 Public Health (Scenarios 15–17)

The three RTI scenarios addressing public health generated 13 responses from stakeholders. These addressed three different domains as indicated below.

Public Health Scenarios			
SCENARIOS	RTI-15	RTI-16	RTI-17
DOMAINS			
2. Information authorization and access		1	4
8. State law restrictions	5		
9. Info use/disclosure	1	1	1
# of Responses	6	2	5
#of Domains	2	2	2

RTI-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 (multi-drug resistant). The patient purchases a bus ticket - the bus ride will take a total of nine hours with two rest stops across several states. State A is made aware of the patient's intent two hours after the bus with the patient leaves. State A now needs to contact the bus company and other states with the relevant information.

General Overview of Stakeholder Business Practice:

The stakeholder respondents included: clinicians, payers, public health agencies, and laboratories. All of the respondents indicated that they would adhere to state laws regarding the disclosure of information for the purposes of public safety, which involved notifying the appropriate units of the Florida Department of Health. The variation in notification policies varied based on the circumstances, the health status of the TB patient, and the process by which the information was communicated from one department to another and the amount of information needing to be disclosed. This scenario resulted in a variety of responses that could create a barrier to HIE and to fulfilling the assurances of the public health system.

Legal Drivers:

The majority of the stakeholders identified the appropriate sections of Florida law that supported their business practices.

Florida Law. Generally, §381.0031(1), F.S., requires health care practitioners practicing in Florida to report certain diseases of public health significance. §64D-3.002(1)(www), F.A.C., specifies that tuberculosis is a reportable disease. Accordingly, the Florida Department of Health would have the general authority to make appropriate disclosures in the interest of public health.⁵³

In addition to the general authority provided under Florida law, Chapter 392 of the Florida Statutes specifically addresses the condition of tuberculosis. §392.55(2), F.S., requires that an individual with active tuberculosis comply with treatment until such time as the individual has been cured. In the event that the individual is not compliant and is deemed to be a threat to the public the Florida Department of Health may request that a warrant be issued to apprehend the individual.⁵⁴ Prior to issuing the warrant a hearing must be held with at least 72 hours notice being provided to the individual.⁵⁵ In the event that individual would not likely appear at a scheduled hearing, §392.57, F.S., authorizes the Florida Department of Health to initiate emergency hold procedures via a petition to the circuit court. If the circuit court issues an emergency hold order the court will direct the sheriff to immediately confine the individual.⁵⁶ §392.65, F.S., requires that information regarding the individual's condition remain confidential. One exception that would allow disclosure of information regarding the individual's condition would be in the event of a medical emergency but only to the extent need to protect the health or life of a named person or group of persons.⁵⁷ This exception could be applicable in the notification of the bus company as indicated in the scenario.

In the event that the individual in the scenario had left the state, the Florida Department of Health would report the matter to other known states via its "Interjurisdictional Tuberculosis Notification System". The communications would be made to the appropriate tuberculosis program coordinators in the applicable states.⁵⁸ All communications would remain confidential.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. 45 C.F.R. §§164.512(a) and 164.512(b) allow for the disclosure of protected health information as "required by law" and for "public health activities". Accordingly the disclosures referenced in this scenario would be appropriate.

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would not conflict with HIPAA.

⁵³ §381.0031(4), F.S.

⁵⁴ §392.55(3), F.S.

⁵⁵ §392.55(4)(a), F.S.

⁵⁶ §392.57(3), F.S.

⁵⁷ §392.65, F.S.

⁵⁸ See, "Florida Department of Health - Technical Assistance: TB 12, October 2004".

RTI-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.

General Overview of Stakeholder Business Practice:

The responding stakeholders, clinicians and community clinics and health centers, indicated that authorization was required in order to access information and that it was important to refer to the state law for the appropriate rules for disclosure. The respondents indicated that it is appropriate to share this information in order to address the public health issues and ensure appropriate care. There was no variation in the responses to this scenario.

Legal Drivers:

The listing of applicable legal drivers were largely absent from the stakeholders responses, although one stakeholder did correctly identify the applicable Florida law governing an information exchange such as the one described in the scenario.

Florida Law. §383.14, F.S., provides for the screening of newborns for certain metabolic, hereditary, and congenital disorders.⁵⁹ §383.14(1)(c), F.S., allows the release of the results to the child's primary care physician such as contemplated in this scenario. §383.14(3)(d), F.S., requires that the Florida Department of Health maintain a confidential registry of cases for the purpose of providing information on the importance of follow up treatment. Additionally, §64C-7.006(2), F.A.C., provides that resulting records be used for the purpose of service delivery and program administration.⁶⁰ Accordingly, appropriate notification to specialty care centers may be permissible if it is for service delivery and program administration.

One example related to the above scenario and relevant to Florida law would be the screening requirement for phenylketonuria (PKU) in newborns. §383.14, F.S., and more specifically, §64C-7.002, F.A.C., requires PKU screening for newborns unless the parents object.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. 45 CFR §164.506(a), would provide for the appropriate disclosure of the individual's protected health information for treatment, payment or health care operations. 45 CFR §164.512(b), would allow the disclosure of the individual's protected health information for public health purposes such as those contemplated in this scenario. Any electronic health information that would be used or disclosed in this scenario would need to comply with the security requirements found in 45 CFR §§164.306, 164.308, 164.310 and 164.312.

⁵⁹§ 64C-7.007, F.A.C., establishes the criteria used to designate which disorders will be screened.

⁶⁰§ 64F-10.008(3), F.A.C., provides the applicable confidentiality standards that are to be followed.

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would not seem to conflict with HIPAA. One potential conflict would be whether the notification of specialty care centers would be consistent with §64C-7.006(2), F.A.C.

RTI-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. 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.

General Overview of Stakeholder Business Practice:

The stakeholder respondents included: state government, clinicians, hospitals, and community clinics and health centers. All of the respondents indicated that patient authorization was required prior to the release of any information, therefore no variation existed.

Legal Drivers:

The stakeholders provided no legal drivers supporting their business practice other than HIPAA.

Florida Law. §397.501(7)(a), F.S., provides that disclosure of information relating to a patient's substance abuse treatment requires the patient's consent. Accordingly, patient information reported from the addiction treatment center to the homeless shelter and the county would need to be authorized by the patient. Excepting the release of information for which re-disclosure is prohibited, the homeless shelter would generally be able to assist the individual in connecting with a relative.

Federal Law. If the treatment facility was considered a "federally assisted drug and alcohol program"⁶¹ the facility would be subject to 42 CFR. Part 2. 42 CFR Part 2, provides a very detailed set of requirements governing the disclosure of the health information of a patient that has been or is currently receiving treatment from a federally assisted alcohol or drug abuse treatment program. 42 CFR §2.53 (b)(2)(i), would allow the addiction center to provide to report information to the county for program reimbursement without the patient's consent.

Additionally, The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are also applicable to the health information exchange contemplated in this scenario. The disclosure for

⁶¹ 42 CFR §2.12, defines a "federally assisted drug and alcohol program" to include, among other things, "A recipient of Federal financial assistance in any form, including financial assistance which does not directly pay for the alcohol or drug abuse diagnosis, treatment, or referral activities;" 42 CFR§ 2.12(3)(i).

payment purposes would be authorized under 45 CFR §164.506(a) for “treatment, payment or health care operations”. The disclosure from the treatment center to the homeless shelter would require the authorization of the patient.⁶² It should be noted that the homeless shelter would be prohibited from re-disclosing any of the patient’s treatment related information.⁶³

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would be more stringent than HIPAA in requiring the patient’s authorization prior to sending information to the county for payment purposes.

⁶² The patient authorization would need to comply with 42 CFR § 2.31.

⁶³ 42 CFR § 2.32.

2.13 State Government Oversight (Scenario 18)

RTI-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 healthcare 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 existing contract with the state university for services of this nature.

General Overview of Stakeholder Business Practice:

The final RTI scenario described a situation that involved state government and the need to exchange information for accountability purposes. This scenario received seven responses that covered three domains of privacy and security:

- Information authorization and access (Domain 2)
- State law restrictions (Domain 8)
- Information use and disclosure (Domain 9)

This scenario was answered by a diverse group of stakeholders, including clinicians, payers, medical schools, community clinics and health centers and RHIOs. The non-clinical stakeholders, payers, medical schools and RHIOs, focused on information use and disclosure policies and the clinical stakeholders focused on user and entity authentication and state law restrictions as part of their business practices.

There was unanimous agreement on the appropriateness of the data-sharing initiative outlined in the scenario. All agreed that the use of health care data for "improving immunization rates and reducing the adverse health consequences of lead" was an acceptable use of the data. It was also noted that "Medicaid generally allows data sharing with Data Use Agreements when the study seeks to improve the administration of the "State Medicaid Plan." This scenario is a common one, with university faculty participating in a state initiative that requires their expertise.

The Florida Department of Health (DOH) already collects and maintains these data through statutory authority or legal agreements. The DOH has processes in place to maintain confidentiality. Medicaid frequently contracts with state universities on issues described in this scenario. However, it was generally agreed that the data are "confidential, no matter what entity or person has possession of it."

In sum, there are no identified barriers to data exchange as long as the appropriate measures and processes are followed.

Legal Driver:

The stakeholders identified various public health laws and HIPAA as the legal drivers to their respective business practices.

Florida Law. The information requested in the scenario would in all likelihood be supplied by at least four different Florida agencies and/or departments, including the Florida Department of Health, the Florida Department of Children and Families, the Florida Department of Education and the Agency for Health Care Administration. All of the aforementioned have deemed themselves to be covered entities under HIPAA with the exception of the Florida Department of Education.

The Florida Department of Health maintains an immunization registry⁶⁴ and a screening program for elevated blood-lead levels.⁶⁵ Patient information contained in the immunization registry is considered confidential excepting access by a licensed health care practitioner.⁶⁶ However §381.0022, F.S., does authorize the exchange of patient information between the Florida Department of Health and the Florida Department of Children and Families for common clients.

§408.05(2), F.S., provides that the Florida Center for Health Information and Policy Analysis shall identify the best available data and coordinate the compilation of extant health-related data and statistics. §408.061(10), F.S., authorizes the Florida Center for Health Information and Policy Analysis to release data to other governmental agencies and parties that contract with the center. All data released would be required to remain confidential. Applied to this scenario the state university would need to enter into a contract pursuant to §408.061(10), F.S., in order to receive the data.

Despite the ability to use or disclose patient information as described above, there does not appear to be any authority that would authorize the disclosure of identifiable patient information in the manner contemplated in the scenario.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. Generally, 45 CFR §164.512(b), would allow protected health information to be utilized without patient consent for public health purposes. Additionally, 45 C.F.R. §164.512(a), would authorize any disclosures of protected health information that is required by law. However, in the case of protected health information of Medicaid applicants and recipients 42 CFR §431.300, restricts the use and disclosure of information to purposes directly connected with the administration of the state Medicaid plan. Without the authorization of the Medicaid applicant or recipient⁶⁷ only de-identified information could be utilized as contemplated in the scenario, although the Agency for Health Care Administration determines whether recipient consent is necessary on a case-by-case basis. It should also be noted that the disclosure of patient information maintained by the Florida Department of Education in school health records would be pursuant to the

⁶⁴ §381.003, F.S.

⁶⁵ §381.985, F.S.

⁶⁶ §381.003(e)(4), F.S.

⁶⁷ 42 CFR 431.306.

requirements of the Family Educational Rights and Privacy Act (FERPA)⁶⁸ as education records are not considered to be protected health information.⁶⁹

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, however, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. In the above scenario Florida law would not conflict with HIPAA with the exception of Medicaid applicant or recipient information. Accordingly, patient information could be disclosed as allowed by Florida law.

2.14 Summary of Critical Observations and Key Issues

Based on the Variations Work Group (VWG) and Legal Work Group (LWG)'s review and analysis of the business practices and domains provided by RTI (and AHCA), there is significant variation in how different stakeholder groups and health care entities operationalize the policies, rules, regulations, and laws governing the exchange of health information. The variation in business practices exist within and across the domains of privacy and security as outlined by HIPAA and other state and federal standards. The basic variation occurs in how a standard is applied, under what circumstances a particular standard applies, and the interpretation of the standard.

Of the 18 scenarios reviewed, 9 presented variations in business practices that created barriers to HIE (RTI 1, 2, 4, 5, 6, 11, 13, 14, and 15). The remaining 9 did not demonstrate enough variation due to limited responses to the scenario or compatibility in business practices.

⁶⁸ 20 U.S.C. §1232(g).

⁶⁹ See definition of "Protected Health Information", 45 C.F.R. §160.103.

SECTION 3

Summary of Key Findings from the Assessment of Variation

3.0 Summary of Key Findings from the Assessment of Variation

3.1 Variations in Business Practices and Policies

In general, the majority of the business practices generated from the review of each scenario addressed policies related to information use and disclosure between health care entities. The VWG and LWG found significant variation in how different stakeholder groups and health care entities operationalize the policies, rules, regulations, and laws governing the exchange of health information. The variation in business practices exist within and across the domains of privacy and security and other state and federal standards.

The basic variation occurs in how a standard is applied, under what circumstances a particular standard applies, and the interpretation of the standard. The assessment identified variations in the following practices related to the private and secure exchange of health information:

1. Requirements regarding verification of patient's or provider's identity
 - a. Provider **seeking** information
 - b. Provider **sending** information
2. Verifying provider's authority to access information
3. Verifying family member or others authority to access information
 - a. Need for Durable Power of Attorney
4. Ability or willingness to transmit urgent or non-urgent data using a fax machine
5. Need for secure encryption of data transmitted between entities
 - a. Healthcare entities vs. Non-Healthcare entities
6. Provider's need to verify that a consent form was completed by patient in the provider's office or in the office where requested information is located or vice versa
7. Use of administrative and physical security safeguards to protect medical records
 - a. Charts locked in secure room with limited card key access
 - b. Facilities protected with electronic surveillance security systems
8. Perceived variation in laws between states when seeking information across state lines
9. Perceived and true variation in how different providers interpret the health information laws.
10. Utilization of electronic health information in the clinical environment.

3.2 Barriers to Health Information Exchange

The variation in business practices often caused barriers to health information exchange that resulted in information not being shared, information not being shared in a timely manner, or information being shared in a non-secure manner. The reason for the variation resulted in barriers that can be characterized as follows:

- A. Inconsistent federal law
- B. Inconsistent state law
- C. Misinterpretation or understanding of HIPAA law
- D. Differences in state and federal laws
- E. Fear of violating the rules or litigation
- F. Longstanding cultural trends and norms within an organization
- G. Differences in organizational policies and practices
- H. Complexity of digital or electronic communication

- I. Insufficient use of electronic health information
- J. Limited or lack of education about HIE and privacy and security laws
- K. Inconsistent laws between states that need to share information

Upon further review of these barriers by the VWG, LWG, and SWG members, it was determined that the barriers were a result of the following central issues: legal issues, regulatory issues, organizational behaviors, technical challenges, and lack of education or public awareness pertaining to health information exchange and HIPAA. Each of these issues represent a proposed solution in the Interim Analysis of Solutions Reports summarized in Section 4 of this report.

3.3 Effective Practices that Protect Privacy and Security

There was very little variation in the business practices related to the use of audit trails and monitoring access to information to avoid unauthorized access and unauthorized modification (Domains 5 and 6) or the disclosure of information in situations warranted to protect the public's health (Domain 9). The limited use of electronic transmission of health information may be the reason for the limited variation across these domains. Very few of the business practices involved the storage or exchange of electronic health information; therefore, the processes for auditing, controlling access, and dissemination for the purposes of public health or crisis management were consistent between groups.

This finding provides evidence that consistency in practices and policies reduces barriers to exchange. The most effective practices were those that were commonly used between entities; however in the case of Florida very few of these common practices related to the private and secure exchange of **electronic** health information. Therefore, as denoted in the next section of this report, considerable attention is made to resolving the legal, regulatory, organizational, technical, and educational barriers to electronic health information exchange.

SECTION 4

Review of Solutions Identification and Selection Process

4.0 Review of Solutions Identification and Selection Process

4.1 Methodology Section

The SWG was the third work group to be convened as part of Florida's Privacy and Security Project. The group was charged with generating solutions to the barriers to HIE identified by the VWG and LWG. The SWG was co-chaired by Kevin Kearns, a member of the Governor's Health Information Infrastructure Advisory Board and Mark Frisse, a special expert in the area of health informatics from Vanderbilt Center for Better Health. It was comprised of 16 members who represented the following stakeholder groups: Florida Health Information Network Grantees, RHIOs, The Florida House of Representatives Health and Families Council, AARP, Florida Osteopathic Medical Association, Institute for Child Health Policy at the University of Florida, Florida College of Emergency Physicians, Florida Department of Health, Associated Home Health Industries of Florida and Florida Alcohol and Drug Abuse Association. Additionally, a representative from the National Conference of Commissioners on Uniform State Laws served on the SWG.

The work group members participated in two work group meetings aimed at developing a framework for identifying and categorizing the solutions to the barriers. In addition to contributing during the two scheduled meetings, the work group members were asked to work with members of their respective organizations or key constituents to identify solutions to the barriers identified and to categorize the solutions identified by the work group. Work group members were provided a template to assist the process (see Appendix 8.4). The SWG was responsible for placing each of the solutions within the proposed framework which was passed on to the Implementation Planning Work Group (IPWG). The IPWG took all of the proposed solutions and prioritized them, determined the feasibility of the solutions and developed an action plan for the solution. The results of this work can be found in the Interim Implementation Plan Report (Deliverable 4) available at: http://ahca.myflorida.com/dhit/Privacy_ss.shtml

4.2 Solutions Framework

The solutions framework developed by the SWG offers a system for categorizing solutions into an organized fashion for further review and consideration of their feasibility for implementation. The purpose of the framework was to help identify solutions with a similar intent and focal point, so that duplicate solutions could be eliminated and similar solutions consolidated upon further review by the IPWG. The solutions categories included legislative, regulatory, organizational or administrative, technology, and education and public awareness solutions. Each one of these categories included a number of solutions that addressed barriers as listed in Section 3.2 of this report.

4.2.1 Legislative Solutions: Solutions in this category involve reviewing, revising, amending, and/or promulgating state or federal laws that impact the exchange of health information, the privacy and security of health information, and the related healthcare diagnosis and treatment activity.

4.2.2 Regulatory Solutions: solutions in this category identify areas where existing rules and regulations may be relaxed, modified, expanded, or clarified to facilitate HIE without the need for legislative action.

4.2.3 Organizational / Administrative Solutions: Solutions in this category address the need to amend, create, and standardize administrative actions, business policies and practices utilized by health care providers at the individual and institutional level.

4.2.4 Technological Solutions: Solutions in this category identify ways in which technology can be used as a solution to the barriers posed by HIE. How can health information technology improve the secure transmission of health information? What technological tools, skills or training may address the barriers to HIE?

4.2.5 Education and Public Awareness Solutions: Solutions in this category address the need for increased public awareness through training and education of consumers, health care providers, government officials, professional associations, employers, public officials, researchers, and educators about the rules governing HIE, the benefits to electronic HIE, and their respective rights and obligations.

SECTION 5

Analysis of Proposed Solutions

5.0 Analysis of Proposed Solutions

5.1 Legislative Solutions

5.1.1 Develop a three-year implementation plan for consolidating statutes related to the exchange of health information that culminates with a resolution to any conflicts between Florida laws and between Florida laws and HIPAA.

General context: There are over 60 Chapters of Florida Statutes which govern the way in which personal health information (PHI) may be shared. In some instances, specific requirements vary greatly depending on the provider type (e.g., hospital vs. physician). In the absence of a statutorily defined uniformed patient consent, many providers are unclear with the specific state provisions that govern the sharing of PHI that are more restrictive than the HIPAA provisions.

Privacy & security domain addressed: State law restrictions.

Types of HIE (clinical, public health, research) addressed: All types.

Stakeholders primarily affected: Health care providers.

HIE barrier(s) addressed: Inconsistent state laws.

Stage of development (planning, implementation): Early stage of planning; previous proposals limited.

Extent to which solution is in use: Health Care Facilities Licensure laws recently reorganized.

Applicability of solution: Might be used as a uniformed national model state law.

Extent of barriers or opposition: Opposition to specific changes possible.

5.1.2 Introduce and adopt legislation to create the Florida Health Information Network (FHIN).

General context: Provide an organizational structure that is charged with establishing privacy and security standards for HIE, creating and maintaining a secure system for exchanging health information between providers and across regions, developing common business associate agreements and other related legal documents, and promotes interoperability between RHIOs.

Privacy & security domain addressed: All.

Types of HIE (clinical, public health, research) addressed: All types.

Stakeholders primarily affected: All

HIE barrier(s) addressed: Differences in organization policies and practices.

Stage of development (planning, implementation): Planning. House Bill 1409 was introduced in the 2006 Legislative Session. On going conversations with IT providers to develop strategic partnership.

Extent to which solution is in use: While many states have projects that serve a portion of state, very few states have developed an overarching design plan to integrate the separate organizations statewide.

Applicability of solution: Could be used as a model for other states and a prototype for a national HIE.

Extent of barriers or opposition: Barriers include: 1) securing the initial investment for the establishment of the network; 2) lack of political support; 3) adopting a business model that will sustain the network over time.

5.1.3 Recommend ways to reconcile differences between state and federal laws relating to preemption and interpretation

General context: Preemption generally refers to the displacement of conflicting or inconsistent state laws by federal laws. The Supremacy Clause (Article VI, section 2) of the United States Constitution states that the Constitution and other federal laws are the "supreme Law of the Land". When there is a conflict between a state law and federal law, the federal law takes precedent or "preempts"--the state law, (e.g. ERISA) unless there is a specific exception (e.g. HIPAA legislation).

Privacy & security domain addressed: State law restrictions.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Differences in state and federal laws.

Stage of development (planning, implementation): Conceptual.

Extent to which solution is in use: Dependent on legislation in question. Preemption analyses have been conducted and are available for reference.

Applicability of solution: May be some applicability across stakeholders although each issue may have unique features to be resolved. Solutions could apply to all stakeholders in other states.

Extent of barriers or opposition: 1) Reluctance on the part of legislators to revisit existing legislation; 2) Competing legislative priorities; 3) Requires a champion to guide the legislation through the legislative process.

5.1.4 Use uniform state consumer banking laws as a template for structuring laws that govern the secure and private exchange of health information.

General context: Use the national and uniform state consumer banking laws and regulations as templates for structuring policy for health information storage and exchange.

Privacy & security domain addressed: All

Types of HIE (clinical, public health, research) addressed: All types.

Stakeholders primarily affected: All stakeholders.

HIE barrier(s) addressed: Inconsistent State and federal laws.

Stage of development (planning, implementation): Conceptual.

Extent to which solution is in use: There have been frequent references to the similarities (in IT adoption) between financial services industry and healthcare industry.

Applicability of solution: Broad applicability if workable.

Extent of barriers or opposition: There have been frequent comparisons made between the data exchange requirements of the health care industry and the banking industry; however some experts believe that the complexity of health care industry make comparisons less useful.

5.1.5 Ensure that the definitions related to health information sharing and exchange that presently exist in statute are consistent with the present meaning in a paper and electronic environment.

General context: Health information has been exchanged in a paper environment until now. The laws may need to be revised to ensure that the meanings of terms are consistent with the capabilities that emerge for HIE in an electronic environment. Ensure that the definitions are consistently applied from one section to the next.

Privacy & security domain addressed: State law restrictions.

Types of HIE (clinical, public health, research) addressed: All types.

Stakeholders primarily affected: All types.

HIE barrier(s) addressed: Inconsistent state laws.

Stage of development (planning, implementation): Conceptual.

Extent to which solution is in use: Words are frequently defined in statute and rule. Need to ensure consistency with existing rules and statutes.

Applicability of solution: Might be used as a model state law.

Extent of barriers or opposition: Some terms have more than one meaning. Many terms in question have already been defined in rule or statute and may have conflicting meanings.

5.1.6 **Revise statutes to provide for the sharing of information between providers in the event of an emergency in which patient is unable to provide written or verbal consent.**

General context: Authorize providers to obtain clinical information from other providers in the case of an emergency where patient is incapacitated or has no legal guardian. There is a potential conflict between HIPAA and hospital statutes, 395 F.S. disallowing the exchange of information without clear patient consent.

Privacy & security domain addressed: User and entity authentication, information authorization and access control, state law restrictions.

Types of HIE (clinical, public health, research) addressed: Clinical.

Stakeholders primarily affected: Health care providers.

HIE barrier(s) addressed: Fear of violating rules, litigation.

Stage of development (planning, implementation): Implementation. Generally by phone or FAX.

Extent to which solution is in use: §397.501 F.S. (substance abuse) authorizes disclosure without consent for emergencies. §456.057 F.S. allows treating physicians to exchange patient information for treatment purposes without prior consent. This same break the glass option is not available to hospitals as specified in §395.3025(4), F.S. Some RHIOs are also developing policies to address this issue.

Applicability of solution: Applicable to all providers who provide emergent care to patients.

Extent of barriers or opposition: No foreseen barriers or opposition.

5.2 **Regulatory Solutions**

5.2.1 **Establish an interstate task force to develop HIE procedures for the exchange of information between states.**

General context: In the event a patient's records need to be transferred between providers in different states, the providers are subject to the laws regulating medical records in the state in which they reside/practice. An interstate task force would allow Florida and its neighboring states to establish guidelines for the private and secure exchange of PHI.

Privacy & security domain addressed: State law restrictions

Types of HIE (clinical, public health, research) addressed: Clinical.

Stakeholders primarily affected: Health care providers.

HIE barrier(s) addressed: Inconsistent laws between states that need to share information

Stage of development (planning, implementation): Early stage; a proposal.

Extent to which solution is in use: Generally ad hoc. eHealth Initiative has established a Gulf Coast Task Force.

Applicability of solution: All participating states.

Extent of barriers or opposition: Access to adequate administrative, legal, and financial resources to implement and sustain task force.

5.2.2 Establish a Florida regulatory task force charged with providing clarification on existing regulations and creating regulations that will advance HIE.

General context: Create a task force to encourage and facilitate the adoption of electronic health information exchange and to address the barriers created by public regulations and/or private policies.

Privacy & security domain addressed: All.

Types of HIE (clinical, public health, research) addressed: All types.

Stakeholders primarily affected: All types – focus on health care providers.

HIE barrier(s) addressed: Limited or lack of education about health information exchange.

Stage of development (planning, implementation): Conceptual.

Extent to which solution is in use: Task force approach is frequently used to guide and direct the implementation of changes in rules and regulations. There are organizations in place with the same or similar mission (e.g. Workgroup for Electronic Data Interchange (WEDI)). The Agency currently holds quarterly meetings of FHIN Grantees to discuss standards, and work on common issues relating to HIE.

Applicability of solution: Applicable to other states and organizations.

Extent of barriers or opposition: Competition for scarce resources (time and dollars) for the establishment of another state level task force.

5.2.3 Establish guidelines/rules that will facilitate the flow of health information between Florida Medicaid program and non-Medicaid providers.

General context: Florida Medicaid typically does not share patient level data with non-Medicaid providers. In order for Medicaid to serve as a participant in a regional health information exchange, new rules and guidelines need to be established authorizing the sharing of health information between Medicaid and non-Medicaid providers.

Privacy & security domain addressed: Information use and disclosure policies.

Types of HIE (clinical, public health, research) addressed: Clinical.

Stakeholders primarily affected: Medicaid and health care providers.

HIE barrier(s) addressed: Differences in state and federal laws and organizational policies and practices.

Stage of development (planning, implementation): Conceptual.

Extent to which solution is in use: The nationally recognized Gold Standard program within Florida Medicaid program could be a model.

Applicability of solution: May affect interpretation by other state Medicaid programs.

Extent of barriers or opposition: Federal regulations may limit what can be accomplished through the establishment of state guidelines. Guidelines from Centers for Medicare and Medicaid Services (CMS) may be more effective.

5.2.4 Apply applicable existing federal regulations that address the secure storage and transmission of data, such as the Food and Drug Administration (FDA) regulations that enforce the establishment and maintenance of secure data repositories.

General context: Require participants in HIE, including individual practitioners to maintain PHI in a secure manner, as is done by the FDA and other federal agencies that store and transmit large amounts of confidential information.

Privacy & security domain addressed: Information transmission security and administrative and physical security of HIE
Types of HIE (clinical, public health, research) addressed: All.
Stakeholders primarily affected: Clinicians, Hospitals and other health care facilities.
HIE barrier(s) addressed: The complexity of digital or electronic communication.
Stage of development (planning, implementation): Conceptual.
Extent to which solution is in use: FDA regulations concerning clinical trial records were issued in April 1999. It is currently being revised. Primary focus is on computerized systems used at clinical sites to collect data. It does not address electronic submissions or methods of their transmission to the FDA.
Applicability of solution: May not be applicable to dynamic HIE; broad applicability if workable.
Extent of barriers or opposition: Potential conflict between existing HIPAA guidance on the physical security of health information.

5.2.5 Create a plan for addressing the sharing of patient health information within states and across states in the event of a natural or manmade disaster resulting in patients being displaced.

General context: Authorize providers to obtain clinical information from other providers in the case of a disaster where the patient is displaced and may or may not have executed consent for HIE.
Privacy & security domain addressed: User and entity authentication, information authorization and access control, state law restrictions.
Types of HIE (clinical, public health, research) addressed: Clinical.
Stakeholders primarily affected: Health care providers.
HIE barrier(s) addressed: Fear of violating rules, litigation.
Stage of development (planning, implementation): Florida College of Emergency Physicians working with federal government to fix the Emergency Medical Treatment and Labor Act (EMTALA).
Extent to which solution is in use: During Hurricane Katrina, HHS Secretary suspended impediments. There is a need for an established plan or rule that authorizes exchange of information.
Applicability of solution: Applicable to all providers.
Extent of barriers or opposition: Need to explore the limitations imposed by the EMTALA laws.

5.2.6 Establish minimal criteria for verifying the identity of providers requesting and transmitting PHI that is consistent across providers.

General context: Define the criteria required to verify the identity of providers participating in a HIE. Different institutions have different processes and policies related to the verification of providers who are seeking or receiving health information on behalf of the patient.
Privacy & security domain addressed: User and entity authentication.
Types of HIE (clinical, public health, research) addressed: Clinical.
Stakeholders primarily affected: Health care providers.
HIE barrier(s) addressed: Complexity of digital or electronic communication.
Stage of development (planning, implementation): Developmental.
Extent to which solution is in use: Health care providers currently use a variety of approaches to verify identity such as caller ID, use of letterhead, or call backs to organization for a separate verification of identify.

Applicability of solution: Applicable to all stakeholders.

Extent of barriers or opposition: Cost and complexity of developing and implementing organization and technical systems that prevents identify fraud while allowing legitimate users to gain ready access to HIE.

5.3 Organizational/Administrative Solutions

5.3.1 Establish a task force to research opportunities to make the electronic capture and exchange of health information reimbursable by Medicaid and under the state employee group health plan.

General context: Create a task force to identify and research opportunities to make the electronic capture and exchange of health information a reimbursable service under Medicaid and other third party payers.

Privacy & security domain addressed: Information transmission and exchange protocols.

Types of HIE (clinical, public health, research) addressed: Clinical.

Stakeholders primarily affected: Payers

HIE barrier(s) addressed: Insufficient utilization of electronic health information due to inadequate funding for implementation of interoperable electronic health records (EHR) systems.

Stage of development (planning, implementation): Conceptual.

Extent to which solution is in use: Government and payers are looking at ways to create incentives for health care providers to use electronic health records in general, but not electronic HIE specifically.

Applicability of solution: Applicable across many payers.

Extent of barriers or opposition: Payers may chose to implement financial incentives that are budget neutral (i.e. disincentives for providers that do not use electronic health records).

5.3.2 Provide financial support for RHIO activities through the joint pursuit of funding opportunities, including grants, fundraising, and government appropriations.

General context: RHIOs are currently using volunteers to establish policies and adopt standards related to HIE. Adequate funding is required to implement recommended technical standards.

Privacy & security domain addressed: Information transmission and exchange protocols.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Insufficient adoption and utilization of electronic health information systems.

Stage of development (planning, implementation): Planning.

Extent to which solution is in use: There are sources of grant funding – state, federal and private.

Applicability of solution: Applicable across RHIOs.

Extent of barriers or opposition: There is a great deal of competition for a limited amount of funding. RHIOs need a financial model that supports long term financial viability.

5.3.3 Produce and distribute standard contracts, business associate agreements (BAAs), and other legal documents required for the establishment of a secure HIE system.

General context: Develop and distribute standard documents for stakeholders to use to facilitate the exchange of health information, to encourage a development of a statewide HIE system, and to legitimize the request of RHIOs seeking this information from provider organizations. If a provider is given multiple BAAs to sign or consider for participation in an HIE, the provider may decide not to participate.

Privacy & security domain addressed: Information use and disclosure policies.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Differences in organizational policies and practices; longstanding cultural trends and norms.

Stage of development (planning, implementation): Planning.

Extent to which solution is in use: Many organizations already distribute model contracts for their members and stakeholders. The Agency currently holds quarterly meetings of FHIN Grantees to discuss standards, and work on common issues relating to HIE. In addition, RHIO documents are posted on the Agency website.

Applicability of solution: Applicable across a variety of organizations and stakeholders.

Extent of barriers or opposition: Some resources would be required to organize and distribute information. A more significant barrier may be the extent to which organizations are willing to change their current practices.

5.3.4 Establish a standardized patient consent form and process that is adopted by the entire health care industry.

General context: The experiences of operational HIE organizations suggest that a uniform process and patient consent form facilitates the exchange of information. When providers have to verify the legitimacy of the document or the patient has to engage in multiple processes, it takes longer for PHI to be exchanged.

Privacy & security domain addressed: Information use and disclosure policies.

Types of HIE (clinical, public health, research) addressed: Clinical.

Stakeholders primarily affected: Health care stakeholders and patients.

HIE barrier(s) addressed: Differences in state and federal laws and organizational policies and practices.

Stage of development (planning, implementation): Early stages of development in Florida.

Extent to which solution is in use: Guidelines are available from national organizations; RHIOs in Florida have begun to establish processes.

Applicability of solution: All states, with some interstate variation due to differences in State laws.

Extent of barriers or opposition: This may require legislation in order to implement and enforce.

5.3.5 Develop quality assurance protocols for the improvement of privacy and security processes within health care organizations.

General context: Utilize quality assurance protocols that offer a rigorous methodology for improving the quality of processes within an organization, to create an environment and culture in healthcare organizations where maintaining privacy and security

standards for PHI is paramount. Privacy and security incidents are discussed and managed and the staff feels comfortable reporting incidents and the institutions implements corrective action plans.

Privacy & security domain addressed: Information audits, Administrative or physical security safeguards.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Fear of violating the rules or litigation, Longstanding cultural trends and norms within an organization, and Differences in organizational policies and practices

Stage of development (planning, implementation): Conceptual.

Extent to which solution is in use: Health care organizations are implementing a similar approach to medical errors through patient safety programs.

Applicability of solution: Applicable to all health care organizations.

Extent of barriers or opposition: A major barrier is the culture of blame that exists in most organizations when it comes to security and privacy breaches. There are also legal ramifications to privacy and security breaches.

5.3.6 Create a Health Information Security Banking Account that allows transactions to occur in a manner similar to ATM transactions.

General context: Create an environment where patients can access their medical records using procedures like those used to conduct banking transactions using an ATM card.

Privacy & security domain addressed: All.

Types of HIE (clinical, public health, research) addressed: Clinical and administrative.

Stakeholders primarily affected: Patients, health care providers and payers.

HIE barrier(s) addressed: Complexity of digital or electronic communication; longstanding cultural trends and norms.

Stage of development (planning, implementation): Conceptual

Extent to which solution is in use: Used in the banking industry e.g. ATM cards

Applicability of solution: Applicable to all health care providers and payers

Extent of barriers or opposition: Provider and patient skepticism of applicability to unique aspects of health care services and sensitive health information. Cost and complexity of developing and implementing necessary infrastructure.

5.4 Technology Solutions

5.4.1 Develop a statewide talent pool of electronic HIE experts who can work together to implement technological solutions without violating the sunshine or revealing corporate trade secrets.

General context: Identify experts that could work to develop technology that supports the development of a private and secure HIE network or system, such as the FHIN.

Privacy & security domain addressed: All domains.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: IT Vendors, CIOs, and privacy and security officers.

HIE barrier(s) addressed: The complexity of digital or electronic communication.

Stage of development (planning, implementation): Early stage, a proposal.

Extent to which solution is in use: The Governor's Health Information Infrastructure Advisory Board has drawn on the talents of many volunteers. The Board is in current discussions with Microsoft and Intel on the development of new technologies.

Applicability of solution: All states.

Extent of barriers or opposition: Funding and other incentives are necessary to retain talent to implement and sustain technological required for security of HIE.

5.4.2 Convene a Florida Health Information Network (FHIN) summit to share technological methodologies that will address the barriers to HIE.

General context: Bring technology providers and users together to discuss and develop new models for HIE activity and recommendations that will advance the utilization of interoperable HIE systems.

Privacy & security domain addressed: All.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Complexity of digital or electronic communication.

Stage of development (planning, implementation): Planning.

Extent to which solution is in use: Agency for Health Care Administration has used a variety of organizations (including, but not limited to the Governor's Health Information Infrastructure Advisory Board) to develop and implement a strategy for the adoption and use of electronic health records and promote the development and implementation of a Florida health information infrastructure.

Applicability of solution: Florida's example could be followed by other states.

Extent of barriers or opposition: Competing priorities, complexity of the healthcare industry.

5.4.3 Utilize tax incentives and other state-supported financing mechanisms for providers to invest in technology that will advance the utilization of private and secure HIE methodologies and systems.

General context: There are few financial incentives related to the adoption of electronic HIE systems, in addition to the fact that utilization of electronic health records by providers is limited. Financial assistance in the development and implementation stages could provide the necessary momentum needed to create a viable network.

Privacy & security domain addressed: Information transmission and exchange protocols.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Complexity of digital or electronic communication.

Stage of development (planning, implementation): Conceptual.

Extent to which solution is in use: Several RHIOs around the state are in varying stages of development funded primarily through grants and donations from the local communities.

Applicability of solution: Applicable to other states.

Extent of barriers or opposition: Limited or lack of education about electronic HIE, the complexity of the industry; limited examples of financial sustainability plans that work; and competing legislative priorities if new types of tax incentives are proposed.

5.4.4 Implement a standard electronic health information system in emergency departments that promotes the use of basic EHR components, such as laboratory reports, prescription writers, Computerized Physician Order Entry (CPOE), electronic transmission of diagnostic images and results.

General context: The nature of emergency care makes it a logical place to implement electronic HIE. Patients typically do not have an established relationship with the health care provider, the severity of the illness or injury may be high, the costs of treatment are high, and the demand for accurate and timely diagnostic information is high. Benefits would include ease of access to critical patient information, improved quality of care, less medication errors, and possibly lower costs.

Privacy & security domain addressed: User and entity authentication, Information transmission security or exchange protocols, and Information audits.

Types of HIE (clinical, public health, research) addressed: All types of HIE are addressed but the demand for clinical data is most critical.

Stakeholders primarily affected: Health care providers.

HIE barrier(s) addressed: Misinterpretation or understanding of HIPAA law, Fear of violating the rules or litigation, Longstanding cultural trends and norms within an organization, Differences in organizational policies and practices, Insufficient use of electronic health information

Stage of development (planning, implementation): Both planning and implementation.

Extent to which solution is in use: Development varies by organization. Some providers have advanced IT systems in place (e.g. digital radiography); however the problem is that the electronic exchange of clinical information between providers is very limited.

Applicability of solution: Solutions to this issue are applicable across the industry.

Extent of barriers or opposition: Cost, complexity, organizational policies and state laws.

5.4.5 Certify biotechnology (biometrics) as an acceptable form of user authentication when verifying providers' authority to access electronic PHI.

General context: Use of IDs and passwords can be easily compromised or forgotten. Biometric authentication refers to technologies that measure and analyze individual physical characteristics for authentication purposes. Examples of physical characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements.

Privacy & security domain addressed: User authentication, access control and physical security.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Complexity of digital and electronic communication.

Stage of development (planning, implementation): Implementation. The use of biometrics is a well established mechanism for authentication and access control.

Extent to which solution is in use: Widely used in a variety of settings.

Applicability of solution: Applicable in a variety of situations.

Extent of barriers or opposition: User resistance may limit large-scale adoption. Up to now, the American public has not accepted a national identification system in any form.

5.4.6 Certify biotechnology (biometrics) as a required method of verifying the identity of patients and matching patient records.

General context: Use of IDs and passwords can be easily compromised or forgotten. Biometric authentication refers to technologies that measures and analyzes individual physical characteristics for authentication purposes. Examples of physical characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements. Patient records would be matched based on the biometric imprint as opposed to an algorithm of demographic variables.

Privacy & security domain addressed: User authentication, access control and physical security.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Complexity of digital and electronic communication.

Stage of development (planning, implementation): Implementation. The use of biometrics is a well established mechanism for authentication and access control.

Extent to which solution is in use: Widely used in a variety of settings.

Applicability of solution: Applicable in a variety of situations.

Extent of barriers or opposition: User resistance may limit large-scale adoption. Up to now, the American public has not accepted a national identification system in any form.

5.4.7 Address digital signature issues by adopting existing guidelines in other industries.

General context: A digital signature is a type of electronic signature. A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document. It may also be used to ensure that the original content of the message or document that has been sent is unchanged.

Privacy & security domain addressed: User and entity authentication, protections against improper modification.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Complexity of digital or electronic communication

Stage of development (planning, implementation): Implemented. Federal law - Electronic Signatures in Global and International Commerce Act. The American Bar Association provides guidelines for the use of digital signatures. In Florida Chapter 668 Florida Statutes authorizes the use of electronic signatures.

Extent to which solution is in use: Not widely used in health care.

Applicability of solution: Applicable to all stakeholders.

Extent of barriers or opposition: Barriers to adoption include technical, representational and privacy issues. Business, cultural and usage barriers to digital signature implementation remain as well.

5.4.8 Identify cost effective, efficient and automated proactive audit mechanisms for use in an electronic health information environment.

General context: Proactive auditing can reveal inappropriate access to electronic health information and potential abuse. Most IT systems include mechanisms to capture system activity including logins, login failures, file accesses and security incidents.

Privacy & security domain addressed: Information authorization and access controls, improper modification, information audits.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Complexity of digital or electronic communication.

Stage of development (planning, implementation): Implemented. The HIPAA Security Rule requires that covered entities implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports (§164.308(a)(1)(ii)(D)).

Extent to which solution is in use: Many healthcare organizations have been struggling with applying the requirements for auditing.

Applicability of solution: Readily available. Most systems include logging mechanisms.

Extent of barriers or opposition: Cost, complexity, and volume of data to analyze.

5.4.9 Establish technological guidelines for “incidental disclosure” when using merge algorithms

General context: Incidental disclosures of protected health information (PHI) occur as a by-product of disclosures permitted under the HIPAA Privacy Rule. Such disclosures are permitted as long as reasonable efforts are undertaken to limit the PHI disclosed to the minimum amount necessary. Merge algorithms are used when matching a patient’s identity across multiple information systems.

Privacy & security domain addressed: Patient and provider identification to match identities across multiple information systems, information authorization and access control.

Types of HIE (clinical, public health, research) addressed: Clinical.

Stakeholders primarily affected: Health care providers.

HIE barrier(s) addressed: Complexity of digital or electronic communication, limited or lack of use of electronic health information.

Stage of development (planning, implementation): Implementation.

Extent to which solution is in use: Health organizations that use record locator services already face this issue.

Applicability of solution: Applicable to stakeholders using record locator services.

Extent of barriers or opposition: Cost and complexity of systems design required to lessen incidental disclosures. Valid records may not be accessible to the clinician when needed as a result of efforts to prevent all incidental disclosures.

5.4.10 Create an electronic process to track incidents in which the wrong patient record is matched.

General context: Each RHIO should create a business process that tracks incidents in which the wrong patient record is matched. The process could accomplish two goals – first it could look at errors over time and use the information to improve the system, second it could mark the record as a “miss” and run the record through additional algorithms to lower the probability of selecting the wrong patient record again.

Privacy & security domain addressed: Patient and provider identification to match identities across multiple information systems.

Types of HIE (clinical, public health, research) addressed: Clinical.

Stakeholders primarily affected: Health care providers.

HIE barrier(s) addressed: Complexity of digital or electronic communication, limited or lack of use of electronic health information.

Stage of development (planning, implementation): Conceptual.

Extent to which solution is in use: Health organizations that use record locator services already face this issue.

Applicability of solution: Applicable to stakeholders using record locator services.

Extent of barriers or opposition: Cost and complexity.

5.4.11 Build HIPAA compliance and state health information laws into the information technology infrastructure of RHIOs

General context: Incorporate Florida law's privacy requirements and HIPAA's rules and standards into the "business rules" that govern the RHIOs' technology systems. Business rules describe the operations, definitions and constraints that apply to an organization's business processes. Following the business rules will ensure that providers follow both state and federal law.

Privacy & security domain addressed: All.

Types of HIE (clinical, public health, research) addressed: Clinical.

Stakeholders primarily affected: Health care providers.

HIE barrier(s) addressed: Complexity of digital or electronic communication, limited or lack of use of electronic health information.

Stage of development (planning, implementation): Conceptual.

Extent to which solution is in use: Business rules are commonly used to drive the decision making process in complex systems.

Applicability of solution: Applicable to all applications and IT systems.

Extent of barriers or opposition: Cost and complexity. There is a great deal of overhead and effort required to maintain the business rules database.

5.5 Education and Public Awareness Solutions

5.5.1 Educate patients on how to access and manage their health information

General context: Attitudes are changing about patient participation in making decisions about their health care. Many patients are unaware of their rights under HIPAA. It is important to educate patients on how to access and manage their health information and the technological tools that are available to assist them.

Privacy & security domain addressed: Information use and disclosure policies.

Types of HIE (clinical, public health, research) addressed: Clinical.

Stakeholders primarily affected: Health care providers and patients.

HIE barrier(s) addressed: Longstanding cultural trends and norms.

Stage of development (planning, implementation): Early stage, a proposal.

Extent to which solution is in use: Both opt in and opt out are in use.

Applicability of solution: All states.

Extent of barriers or opposition: Competing priorities, avoiding legalese.

5.5.2 Create a Florida Health Information Network (FHIN) speakers bureau to advocate for the advancement of electronic HIE.

a. Appoint HIE Awareness Committee to raise awareness among influential stakeholders

b. Encourage RHIOs and local communities to develop legislative briefs and agendas that raise the awareness of electronic HIE

General context: Developing a group of individuals to advocate for electronic HIE would help to communicate the advantages of HIE to a broader audience and increase the rate of adoption.

Privacy & security domain addressed: Information use and disclosure

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Limited or lack of education about HIE and privacy and security laws.

Stage of development (planning, implementation): Planning.

Extent to which solution is in use: There are some organizations advocating for HIE e.g. the Governor's Health Information Infrastructure Advisory Board, Healthcare Information Management and Systems Society, Workgroup for Electronic Data Interchange.

Applicability of solution: Applicable to other states.

Extent of barriers or opposition: Achieving agreement on main message and competing priorities for time and attention of volunteers.

5.5.3 **Host focus groups or information sessions with influential stakeholders to inform them of the national, state and local activities in the area of electronic HIE as a means of building support for state and local initiatives.**

General context: Organizing focus groups or information sessions within a political or social group can serve as a vehicle for educating and informing the public of issues related to HIE. It can foster buy-in and motivate key stakeholders to support HIE initiatives.

Privacy & security domain addressed: Information use and disclosure policies

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Limited or lack of education about HIE and limited or lack of use of electronic health information.

Stage of development (planning, implementation): Conceptual.

Extent to which solution is in use: Used in other venues.

Applicability of solution: Applicable to other states.

Extent of barriers or opposition: Requires trained facilitators, influential stakeholders might not be available for time consuming process and findings cannot be generalized unless balanced representation of all view points achieved.

5.5.4 **Establish web site or blog site to provide updates on state activities.**

General context: Web site can be used to carry the message of the value of electronic HIE to a wider audience and it can be used to communicate Project and program progress.

Privacy & security domain addressed: Information use and disclosure

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Limited or lack of education about HIE and privacy and security laws.

Stage of development (planning, implementation): Implemented.

Extent to which solution is in use: The Agency for Health Care Administration has content on its web site devoted to the development and implementation of a strategy for the adoption and use of electronic health records

(<http://ahca.myflorida.com/dhit/index.shtml>). The website includes a page on the Florida Privacy and Security Project.

Applicability of solution: Very applicable to all stakeholders.

Extent of barriers or opposition: Relatively low - cost of hosting a web site and developing and maintaining content.

5.5.5 Implement a public awareness and education campaign that will provide accurate information about electronic health records, risks associated with paper charts, and the positive aspects of electronic health information.

General context: Create a communication plan that utilizes a variety of communication channels to deliver the message that information technology is an enabler in the healthcare industry and we should encourage the development of electronic HIE.

Privacy & security domain addressed: Information use and disclosure

Types of HIE (clinical, public health, research) addressed: Clinical.

Stakeholders primarily affected: All, including the general public.

HIE barrier(s) addressed: Longstanding cultural trends and norms, limited or lack of education about HIE and privacy and security laws.

Stage of development (planning, implementation): Implemented.

Extent to which solution is in use: There are a variety of messages in both the professional and popular media extolling the virtues of electronic HIE.

Applicability of solution: Applicable to all stakeholders.

Extent of barriers or opposition: Need adequate funding to be effective.

5.5.6 Implement a public awareness and education campaign that clarifies and addresses the inconsistent interpretation of HIPAA and defines health information exchange related terms as they relate in either the paper or electronic environment.

General context: One of the findings in *Florida's Interim Assessment of Variations Report* was that many providers misinterpret the HIPAA Rules and Standards. Frequently they have an overly restrictive interpretation of what the rules and regulations require and in turn restrict the flow of patient information between stakeholders.

Privacy & security domain addressed: State law restrictions.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Limited or lack of education about HIE and privacy and security laws.

Stage of development (planning, implementation): Implementation.

Extent to which solution is in use: There are a variety of organizations working to educate stakeholders on HIPAA. They include, but are not limited to, health care professional organizations, the Centers for Medicare and Medicaid Services, the Office for Civil Rights and the Workgroup for Electronic Data Interchange.

Applicability of solution: Applicable to all states.

Extent of barriers or opposition: Competing priorities, employee turnover.

5.5.7 Encourage the utilization of existing mechanisms for authorizing family members and others access to another's PHI, such as the durable power of attorney, health care surrogate, and living wills. Ensure that these documents authorize access to PHI when and how the patient desires.

General context: Long term care providers consistently utilize the power of attorney document with their patients. Other health care providers are less consistent in their application with their patients.

Privacy & security domain addressed: State law restrictions. Information authorization

Types of HIE (clinical, public health, research) addressed: Clinical information.

Stakeholders primarily affected: Health care providers.

HIE barrier(s) addressed: Inconsistent state and federal laws.

Stage of development (planning, implementation): Conceptual stage.

Extent to which solution is in use: Florida Statutes provide for a health care surrogate §765.201 F.S. Designation of Health Care Surrogate.

Applicability of solution: Could be used as a model for other states and the federal government.

Extent of barriers or opposition: Funding, competing priorities, and consumer resistance.

5.5.8 Encourage adoption and utilization of defined minimal criteria for authorizations related to the access and use of PHI.

General context: Define the criteria required to authorize an individual to access and use confidential patient information. After identity is established, it must be determined that the individual has the authority to access information. This authority is granted through patient consent, legislation, organizational policy, and role.

Privacy & security domain addressed: Information authorization and access control.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Complexity of digital or electronic communication.

Stage of development (planning, implementation): Implementation.

Extent to which solution is in use: Access control measures are well established in the administration of information technology networks and applications.

Applicability of solution: Applicable to all health care providers and payers

Extent of barriers or opposition: Concepts of access control are well accepted. Administration across RHIOs may add some administrative complexity.

5.5.9 Encourage adoption and utilization of standardized encryption methods.

General context: Encryption is the process of taking a document or message and scrambling it so that it cannot be read by unauthorized individuals.

Privacy & security domain addressed: Information transmission security or exchange protocols for information that is being exchanged over a network.

Types of HIE (clinical, public health, research) addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: The complexity of digital or electronic communication.

Stage of development (planning, implementation): Implemented. Encryption protocols are well established.

Extent to which solution is in use: In use in a variety of healthcare organizations.

Applicability of solution: Applicable to all stakeholders.

Extent of barriers or opposition: Cost, complexity, incompatible encryption techniques and authentication issues.

SECTION 6

National-Level Recommendations

6.0 National-Level Recommendations

The following solutions have been identified as recommendations that may benefit from a national implementation strategy in addition to the local and state efforts proposed by Florida's Privacy and Security Project team. The proposed national lead for each solution is the entity that may be best suited to advise or coordinate the implementation of the solution at the national level.

Solution Analysis Ref. #	Description of National-Level Recommendation	Proposed National Lead for Solution
Leg. 5.1.3.	Recommend ways to reconcile differences between state and federal laws relating to preemption and interpretation.	National Conference of Commissioners on Uniform State Laws (NCCUSL)
Leg. 5.1.4.	Use uniform state consumer banking laws as a template for structuring laws that govern the secure and private exchange of health information.	NCCUSL, The Medical Banking Project
Reg. 5.2.1.	Establish an interstate task force to develop HIE procedures for the exchange of information between states.	Office of the National Coordinator (ONC), National Governor's Association (NGA)
Reg. 5.2.3.	Establish guidelines/rules that will facilitate the flow of health information between Florida Medicaid program and non-Medicaid providers.	Center for Medicare and Medicaid Services (CMS)
Reg. 5.2.4.	Apply applicable existing federal regulations that address the secure storage and transmission of data, such as the Food and Drug Administration (FDA) regulations that enforce the establishment and maintenance of secure data repositories.	ONC, Food and Drug Administration (FDA)
Reg. 5.2.5.	Create a plan for addressing the sharing of patient health information within states and across states in the event of a natural or manmade disaster resulting in patients being displaced.	ONC, Federal Emergency Management Administration (FEMA), NGA
Reg. 5.2.6.	Establish minimal criteria for verifying the identity of providers requesting and transmitting PHI that is consistent across providers.	ONC, National Health Information Network (NHIN)
Org. 5.3.6.	Create a Health Information Security Banking Account that allows transactions to occur in a manner similar to ATM transactions.	ONC, The Medical Banking Project

Solution Analysis Ref. #	Description of National-Level Recommendation	Proposed National Lead for Solution
Tech. 5.4.4.	Implement a standard electronic health information system in emergency departments that promotes the use of basic EHR components, such as laboratory reports, prescription writers, Computerized Physician Order Entry (CPOE), electronic transmission of diagnostic images and results.	ONC, American Hospital Association (AHA)
Tech. 5.4.5.	Certify biotechnology (biometrics) as an acceptable form of user authentication when verifying providers' authority to access electronic PHI.	ONC, NHIN
Tech. 5.4.6.	Certify biotechnology (biometrics) as a required method of verifying the identity of patients and matching patient records.	ONC, NHIN
Tech. 5.4.7.	Address digital signature issues by adopting existing guidelines in other industries.	ONC, NHIN
Tech. 5.4.8.	Identify cost effective, efficient and automated proactive audit mechanisms for use in an electronic health information environment.	ONC, NHIN
Tech. 5.4.9.	Establish technological guidelines for "incidental disclosure" when using merge algorithms	ONC, NHIN
Tech. 5.4.10.	Create an electronic process to track incidents in which the wrong patient record is matched.	ONC, NHIN
EPA 5.5.5.	Implement a public awareness and education campaign that will provide accurate information about electronic health records, risks associated with paper charts, and the positive aspects of electronic health information.	ONC, NGA
EPA 5.5.6.	Implement a public awareness and education campaign that clarifies and addresses the inconsistent interpretation of HIPAA and defines health information exchange related terms as they relate in either the paper or electronic environment.	ONC, NGA
EPA 5.5.8.	Encourage adoption and utilization of defined minimal criteria for authorizations related to the access and use of PHI.	ONC, NHIN
EPA 5.5.9.	Encourage adoption and utilization of standardized encryption methods.	ONC, NHIN

SECTION 7

Conclusions and Next Steps

7.0 Conclusions and Next Steps

The assessment of variation and analysis of solutions were critical steps in the process of developing feasible action plans for the Final Implementation Plan Report. The Final Implementation Plan Report includes eleven work plans comprised of the primary goals and objectives of the Florida Privacy and Security Project. At the onset of the project, Florida aspired to collect information from key stakeholders that could be used to overcome the barriers to developing and maintaining a private and secure electronic health information exchange infrastructure. The goal of collecting useful and operational information was achieved. The data was then used to create a vision, mission, and several core goals related to electronic health information exchange in Florida. This strategic framework is outlined in the Final Implementation Plan Report, which also includes details on how Florida intends to meet its goals and objectives.

For more information about the Florida Privacy and Security Project and copies of the referenced reports visit Florida's Agency for Health Care Administration's website at: http://ahca.myflorida.com/dhit/Privacy_ss.shtml.

SECTION 8

Appendices

8.0 Appendices

8.1 Florida Scenarios

In addition to the 18 scenarios provided by RTI, Florida created four scenarios that target issues important to Florida and its development of a statewide health information infrastructure, specifically Medicaid, RHIO HIEs, and the utilization of personal health records. The Florida scenarios were circulated and analyzed with the RTI scenarios. There were a total of 17 responses to Florida scenarios, representing four different domains:

- User and entity authentication
- Information authorization and access
- Patient and provider identification
- Information use and disclosure

The following is the legal analysis of the Florida scenarios.

8.1.1 FL-1: Medicaid Scenario

FL-1. Medicaid Scenario

A physician treating a former Medicaid patient at a rural health clinic needs information on the patient's congestive heart failure treatment regimen. The doctor decides to access the Medicaid EHR. The patient gives oral consent.

General Overview of Stakeholder Business Practice:

The responding stakeholders, to varying degrees, indicated that unless the physician was a current Medicaid provider either written consent or a valid patient password (for an electronic health record) would be required.

Legal Driver:

The stakeholders identified HIPAA and/or Federal Medicaid law as the applicable legal drivers.

Florida Law. One crucial factor in determining whether or not the physician in the scenario may access the Medicaid EHR would be the physician's Medicaid provider status. If the physician was a participating Medicaid provider he/she would have entered into a provider agreement with the Agency for Health Care Administration pursuant to §409.907, F.S. Among the requirements for participating Medicaid providers would be the requirement to safeguard the use or disclosure of information of current or former Medicaid recipients.⁷⁰ Accordingly, a currently enrolled Medicaid provider would be able to access the information.

In the event that the physician was not a currently enrolled Medicaid provider, the physician would need to obtain the written authorization of the patient (see below).

⁷⁰ §409.907(3) (d), F.S.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. 45 CFR §164.502(a)(1) (ii) and 45 CFR §164.506 (c)(2), would allow the exchange of information requested in the scenario, regardless of the physician’s status as a Medicaid provider. However, the confidentiality requirements under the Medicaid program would not allow for the exchange of information as contemplated in the scenario if the physician was not an enrolled Medicaid provider.

42 CFR §§431.300 - 307, provide the requirements for safeguarding of patient information. However, these requirements are only applicable to applicants or Medicaid recipients.⁷¹ 42 CFR §431.306(d), would allow the release of an applicant’s or recipient’s information upon the authorization of that individual, unless emergency circumstances did not permit obtaining authorization prior to release.⁷²

In the specific situation contemplated in this scenario, the Agency for Health Care Administration would require that the former Medicaid patient provide written authorization prior to the release of the information unless it was an emergency as provides under the federal regulations cited *supra*.

Florida Law and HIPAA. While HIPAA would normally preempt a contrary state law, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. It is likely that Florida law could be considered more stringent than HIPAA and therefore require the patient’s authorization prior to disclosure. Additionally, both Federal Medicaid law and Florida Statutes pertaining to Medicaid would also be more stringent than HIPAA.

⁷¹ 42 CFR §431.300(a).

⁷² The regulation is silent as to whether oral or written consent would be required. However, it is the policy of the Agency for Health Care Administration to require written authorization to mitigate the risk of inappropriate disclosure.

8.1.2 FL-2: RHIO Scenario

FL-2. RHIO Scenario

A participating physician of a RHIO is sued for malpractice. The physician asks the RHIO for documentation of records viewed on three specific dates and times.

General Overview of Stakeholder Business Practice:

The responding stakeholder indicated that it would be appropriate to release the requested information to the physician.

Legal Drivers:

The stakeholder listed HIPAA as the applicable legal driver.

Florida Law. In order to determine applicable Florida law to be applied in this scenario the following preliminary questions, at a minimum, would need to be answered. Does the RHIO maintain information on a clinical record or does it merely point an authorized user to the correct record host? What records are being requested? Is the physician in the scenario requesting documentation as to records created by him/her or is the physician requesting documentation as to records created by other providers? Is the physician requesting documentation related to other authorized users of the RHIO who may have viewed the physician's records?

§456.057(1), F.S., provides that any health care practitioner who generates a medical record after making a physical or mental examination is to be considered the "records owner".⁷³ The aforementioned statute also provides that a health care practitioner's employer may be deemed as the records owner if so designated in an employment contract or agreement between the provider and the employer. Accordingly, the provider should be allowed access to information regarding a clinical record he/she created.

If the physician in the scenario were to need access to the records of another provider to obtain the required documentation, §766.204, F.S., would allow for such a disclosure during the malpractice pre-suit investigation phase.⁷⁴ In the event that the physician was trying to access such records after the filing of a lawsuit, then the physician may need to obtain them via a subpoena.⁷⁵

In the event the physician in the scenario is requesting information as to what other persons or entities, via the RHIO, viewed a medical record they created, the physician should have access to such information. §456.057(12), F.S., requires that all record owners maintain a record of all disclosures of information contained in the medical record. Accordingly, if the RHIO in this scenario were maintaining the physician's medical record the physician would have been required to implement a procedure with the RHIO regarding third party disclosures.

⁷³ §456.057(2), F.S., provides a listing of practitioners and employers, such as certified nursing assistants and pharmacies that are excluded from the term "records owner".

⁷⁴ §766.106, F.S., requires a pre-suit screening process prior to the initiation of a legal action for medical malpractice.

⁷⁵ Fla.R.Civ.P. 1.351.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. 45 CFR §164.506(c)(1), would allow the physician in this scenario to access his/her own records for treatment, payment or health care operations without the consent of the patient.⁷⁶ The Physician, generally, would need an authorization pursuant to 45 CFR §164.508, or a valid subpoena as authorized under 45 CFR §164.512(e), to access the records of another physician for the purposes of defending a lawsuit.⁷⁷

Additionally, the covered entities participating in the RHIO would need to require that any protected health information used or disclosed via the RHIO be subject to the applicable provisions of 45 CFR §§164.306, 164.308, 164.310 and 164.312.⁷⁸ Accordingly, the RHIO should have appropriate audit mechanisms in place to address the inquiry contemplated in this scenario.⁷⁹

Florida Law and HIPAA. While HIPAA would normally preempt a contrary state law, 45 C.F.R. §160.203(b), provides an exception for state laws that are more stringent than HIPAA. The application of Florida law in this scenario would not, generally, conflict with HIPAA.

⁷⁶ 45 CFR §164.501, includes in paragraph 4 of the definition of “Health Care Operations” the conducting or arranging of legal services.

⁷⁷ 45 CFR §164.506(c)(4), authorizes a covered entity to disclose protected health information to another covered entity for health care operations of the entity receiving the information, if each entity has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is limited to purposes listed in paragraphs 1 and 2 in the definition of “Health Care Operations”. The arranging of legal services is mentioned in paragraph 4 of the definition and therefore disclosure would not be appropriate.

⁷⁸ It is assumed that the RHIO would be a “business associate” of all the providers participating in the RHIO pursuant to 45 CFR §164.502(e) and 45 CFR §164.308(b)(1).

⁷⁹ 45 CFR §164.312(b).

8.1.3 FL-3: RHIO Scenario

FL-3. RHIO Scenario

A participating employer of a RHIO wants to obtain aggregate data from the RHIO to compare quality of health care providers and payers. The employer will fund the project so that the data can be released without disclosing any PHI. However, facilities, physicians, and payers would be identified.

General Overview of Stakeholder Business Practice:

The responding stakeholders generally indicated that data could be disclosed if the data was de-identified. Other stakeholders also indicated the need for a data use agreement.

Legal Drivers:

The responding stakeholders identified HIPAA and applicable Medicaid law in general.

Florida Law. A strict reading of §395.3025(4), F.S., and §456.057(7)(a), F.S., would prohibit the release of patient information contemplated in the scenario. Although the scenario indicates PHI would not be disclosed, the aforementioned statutes apply to patient “medical records” as a whole and do not address the concept of de-identification. Both statutes would, therefore, require the authorization of the patients prior to the release of information.

Interestingly, §408.05, F.S., provides that the Florida Center for Health Information and Policy Analysis will collect data similar to the data being requested in the scenario. In the event that the request made in the scenario was made to a RHIO maintained by the state of Florida, the result may be different. §408.061(10), F.S., authorizes the Florida Center for Health Information and Policy Analysis to release data to other governmental agencies and parties that contract with the Center.⁸⁰ All data released would be required to remain confidential. Applied to this scenario the employer, having entered into the appropriate data use agreement, would be able to receive at least some of the data contemplated in the scenario.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. 45 CFR §164.502(d)(2), allows for the use of health information that has been appropriately de-identified in accordance with the applicable requirements of 45 CFR §164.514. The situation contemplated in the scenario would appear to comply with the appropriate de-identification requirements. However, in the case of using de-identified Medicaid data a data use agreement with the State Medicaid Agency may be required. 42 CFR §431.306(b), limits the release of Medicaid recipient or applicant information to persons or agencies that are subject to the same confidentiality requirements as the State agency that administers the Medicaid program.

Florida Law and HIPAA. While HIPAA would normally preempt a contrary state law, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. Applied to this scenario, Florida law would be more stringent than HIPAA. Additionally, Federal Medicaid law and Florida statutes pertaining to Medicaid would also be more stringent than HIPAA.

⁸⁰ §408.061(8), F.S., would not authorize the release of information identifying a provider or payer.

8.1.4 FL-4: Personal Health Record Scenario

FL-4. Personal Health Record Scenario

Hurricane XYZ threatens coast and an evacuated home health patient at a shelter needs insulin, oxygen and heart medicine. The patient has a PHR as a service provided by her HMO but cannot recall the password. A nurse working at the shelter asks her assistant to call the HMO to obtain access to the patient's PHR.

General Overview of Stakeholder Business Practice:

The responding stakeholders generally indicated that they would attempt to obtain access to the patient's PHR password by contacting the HMO and providing either the patient's oral or written authorization. The stakeholders also indicated that they believed the exigent circumstances would have at least some bearing as to whether the HMO would provide the password.

Legal Drivers:

The stakeholders indicated that the appropriate legal drivers would be HIPAA and/or non-specific state laws related to emergency situations.

Florida Law. The release of the password by the HMO to the nurse at the shelter would likely be dependent on the confidentiality policies⁸¹ of the HMO in question. Certain conditions that may be indicated in a patient's medical record may, arguably, be released upon the written authorization of the patient.⁸² Therefore it is likely that the HMO would request the authorization of the patient prior to releasing the password. It should be noted that the patient in this scenario would likely be considered a special needs patient pursuant to §252.355(1), F.S., who would have had the opportunity, via the patient's home health provider, to confidentially register with the local emergency management agency. Normally, such registration would include the provision of information related to life-sustaining equipment such as oxygen and life-sustaining medications. Additionally, the registration would also provide authorization for the use of such information by emergency personnel such as the shelter nurse.

Federal Law. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104–191 and its implementing regulations found at 45 CFR Parts 160, 162 and 164 are applicable to the health information exchange contemplated in this scenario. The HMO would be considered a covered entity under 45 CFR §160.103 and would therefore be required to comply with the relevant provisions of 45 CFR Part 164. 45 CFR §164.502(a)(1)(ii), and 45 CFR §164.506(c)(2), would authorize the disclosure of protected health information to the nurse for the treatment activities contemplated in this scenario.⁸³ Additionally, 45 CFR §164.502(a)(1)(i), would allow the disclosure to the patient who was at the hurricane shelter.

⁸¹ §641.54(5)(c), F.S., requires HMOs to provide each subscriber, upon request, policies and procedures related to the confidentiality and disclosure of the subscriber's medical records.

⁸² See for example, §641.59, F.S., for psychotherapeutic records. It should be noted that this statute provides for the confidential maintenance of a patient's medical record but does not specifically indicate that an authorization would be required.

⁸³ The release of psychotherapy notes would require the patient's authorization pursuant to 45 CFR §164.508(a)(2).

Florida Law and HIPAA. HIPAA would normally preempt a contrary state law, 45 CFR §160.203(b), provides an exception for state laws that are more stringent than HIPAA. As applied to this scenario, Florida law could be considered more stringent and therefore require the patient's authorization prior to disclosure.

8.2 Work Group Members

8.2.1 Variations Work Group Members

Peter Greaves, Chair and Member of Governor’s Health Information Infrastructure Advisory Board (GHIIAB)

FHIN Grant & RHIO representatives

Ron Fucci
Allen Byington for Dan Kaelin
Huy Nguyen

Department of Health

David Taylor
James Huber

Florida Academy of Family Physicians

Tad Fisher

Florida Association of Community Health Centers

Andrew Behrman

Florida Dental Association

Dr. Alan Friedel for Joe Anne Hart

Florida Hospital Association

Katherine Holzer

Florida Nurses Association

Mike Nilsson for Barbara Lumpkin

Florida Health Care Association

Tony Marshall

Florida Pharmacy Association

Michael Jackson

Florida VA

James M. Lieupo

Florida Medicaid

Alan Strowd for Dyke Snipes

Health Information Management Student

Cymeia Hill

Humana

Harry Spring

National Conference of Commissioners on Uniform State Laws

Grant Callow

8.2.2 Legal Work Group Members**Ronald Burns, D.O., Chair and Member of Governor's Health Information Infrastructure Advisory Board (GHIAB)****FHIN Grant Awardees/RHIO/HIE representatives**

Jan Gorrie
Sandra Greenblatt

Florida Hospital Association

Bill Bell, General Counsel

Florida Medical Association

John Knight, General Counsel
Jeff Scott, Associate General Counsel

Florida Department of Health, Board of Medicine

Larry McPherson, Executive Director

Florida Department of Health, Board of Dentistry

Sue Foster, Executive Director

Florida Department of Health

Rodney Johnson for Tim Cerio, General Counsel

Florida Department of Children and Families

Carolyn Dudley, Privacy Officer, Office of Civil Rights

Florida Department of Elder Affairs

Barbara Crosier, General Counsel

Florida Office of Insurance Regulation

Amanda Parnell for Steve Parton/Dennis Threadgill

Agency for Health Care Administration

James Bruner, Director, Bureau of Compliance and Strategy

Agency for Health Care Administration

Bill Roberts, Acting General Counsel

National Conference of Commissioners on Uniform State Laws

Grant Callow

Blue Cross Blue Shield of Florida

Steven Smith

United Health

Leslie Dughi

Health Law Attorney

Wendy Hansen

8.2.3 Solutions Work Group Members

Kevin Kearns, Co-Chair and Member of Governor's Health Information Infrastructure Advisory Board

Dr. Mark Frisse, Co-Chair, Vanderbilt Center for Better Health

FHIN Grant Awardees/RHIO/HIE representatives

Christine Isham

Laura Kolkman

Patricia MacTaggart

Catherine Peper

Florida House of Representatives Health and Families Council

Amber Bell for Mary Pat Moore

AARP

Lori Parham

National Conference of Commissioners on Uniform State Laws

Grant Callow

Florida Osteopathic Medical Association

Linda Delo, D.O.

Institute for Child Health Policy, University of Florida

Steve A. Freedman, Ph.D.

Associated Home Health Industries of Florida

Gene J. Tischer

Florida College of Emergency Physicians

David M. Siegel, MD JD FACEP FACP

Florida Department of Health

Rodney Johnson for Tim Cerio, General Counsel

Florida Department of Health, Bureau of HIV/AIDS

Pam Lowell for Tom Liberti

Florida Alcohol and Drug Abuse Association

Laurence Roberts and Pam Haines, Operation PAR, for John Daigle

8.2.4 Steering Committee Members

Governor's Health Information Infrastructure Advisory Board, (GHIIAB)

Privacy and Security Project Steering Committee

Chairman

- **W. Michael Heekin, Chairman of the GHIIAB Board and Special Advisor to the Governor**

Members

- **Carmen Aceves-Blumenthal, Pharmacist, McKesson Medication Management**
- **Robert G. Brooks, MD, Associated Dean for Health Affairs, Florida State University**
- **Ronald R. Burns, DO, Private Practitioner, and Past President, Florida Osteopathic Medical Association**
- **Raymond F. Caron, MD, JD, Pediatrician in Private Practice**
- **Brian O. Coleman, DMD, Dentist and Trustee, Florida Dental Association**
- **Jeannette W. Ekh, Chief Information Officer, Blue Cross Blue Shield of Florida**
- **Peter D. Greaves, Senior Enterprise Architect, HCA, Inc.**
- **Kevin S. Kearns, Chief Executive Officer, Health Choice Network**
- **Rhonda M. Medows, MD, Commissioner, Georgia Department of Community Health and former Secretary, Agency for Health Care Administration**
- **Linda E. Moody, Ph.D, Professor University of South Florida College of Nursing**
- **James S. "Sandy" Phillips, Chief Operating Officer, Tenet Account, Perot Systems**
- **Robert G. Reese, Senior Technology Consultant, Healthcare Systems**

8.2.5 HISPC Stakeholder Group Participation

Stakeholder Group	HISPC WORK GROUPS					OUTREACH TO STAKEHOLDERS		
	Steering Committee (X)	Variations Work Group (X)	Legal Work Group (X)	Solutions Work Group (X)	Implementation Planning Work Group (X)	Stakeholders providing input to variations assessment (N)	Stakeholders providing input to solutions development and evaluation (X)	Stakeholders providing input to implementation planning (X)
Clinicians	X	X		X	X	34	X	X
Physicians and Physicians Groups	X	X	X	X	X	12	X	X
Federal Health Facilities		X				7		
Emergency Medicine		X		X		1	X	
Hospitals / Health Systems	X	X	X		X	11		X
Community Clinics and Health Centers	X	X				13		
Mental Health and Behavioral Health				X		1	X	
Long Term Care Facilities and Nursing Homes						4		
Homecare and Hospice				X		1	X	

Stakeholder Group	HISPC WORK GROUPS					OUTREACH TO STAKEHOLDERS		
	Steering Committee (X)	Variations Work Group (X)	Legal Work Group (X)	Solutions Work Group (X)	Implementation Planning Work Group (X)	Stakeholders providing input to variations assessment (N)	Stakeholders providing input to solutions development and evaluation (X)	Stakeholders providing input to implementation planning (X)
Laboratories						9		
Pharmacies / Pharmacy Benefit Managers	X	X				1		
Safety Net Providers		X			X	1		X
Professional Associations and Societies		X	X			8		
Quality Improvement Organizations					X	1		X
Medical and Public Health Schools / Research	X			X	X	3	X	X
Public Health Agencies or Departments		X	X	X	X	19		X
Medicaid / Other State Government	X	X	X	X	X	3	X	X
County Government					X	1		X

Stakeholder Group	HISPC WORK GROUPS					OUTREACH TO STAKEHOLDERS		
	Steering Committee (X)	Variations Work Group (X)	Legal Work Group (X)	Solutions Work Group (X)	Implementation Planning Work Group (X)	Stakeholders providing input to variations assessment (N)	Stakeholders providing input to solutions development and evaluation (X)	Stakeholders providing input to implementation planning (X)
Laboratories						9		
Pharmacies / Pharmacy Benefit Managers	X	X				1		
Safety Net Providers		X			X	1		X
Professional Associations and Societies		X	X			8		
Regional Health Information Organizations		X	X	X	X	5	X	X
Payers	X	X	X	X	X	6	X	X
Individual Consumers		X	X			2		
Consumer Organizations and Advocates				X	X	3	X	X

Stakeholder Group	HISPC WORK GROUPS					OUTREACH TO STAKEHOLDERS		
	Steering Committee (X)	Variations Work Group (X)	Legal Work Group (X)	Solutions Work Group (X)	Implementation Planning Work Group (X)	Stakeholders providing input to variations assessment (N)	Stakeholders providing input to solutions development and evaluation (X)	Stakeholders providing input to implementation planning (X)
Employers					X	1		X
Law Enforcement and Correctional Facilities						0		
Legal Counsel / Attorneys		X	X	X	X	14	X	X
Health Information Management organizations						0		X
Privacy and Security experts / Compliance officers			X		X	1		X
Health IT consultants	X				X	1		X
Electronic Health Records experts						0		
Technology Organizations / Vendors						0		
Other (specify): National Conf. of Comm. on Uniform Laws (NCCUSL)		X	X	X	X	1		

8.3 Variations Template

Privacy and Security Project Business Practice Template

RTI-Scenario title

(Actual RTI scenario listed in this field)

*Please use attached coding sheet to complete this portion of the form.
Select only one code for each category.*

Stakeholder Group:		Domain Addressed:		Classification of Business Practice:	
---------------------------	--	--------------------------	--	---	--

Business Practice:	
Assumptions made upon review of the scenario:	
Long Description of Business Practice:	
Business Policy to Support Practice:	
Legal Driver Behind Policy?	
Statutory Reference:	

Coding Sheet for Privacy and Security Business Practices Template

For consistency, please refer to the following standard definitions when reviewing each scenario

Assumption – A belief or logical construct regarding the facts or situation that may be the basis for a decision or plan of action, often assumptions are implicit, i.e. often left unsaid.

Business Practice – Organizational practices that are implemented to address the needs of the business in meeting organizational goals, meeting legal requirements and remaining profitable.

Legal Driver – Legal or statutory requirement, an authorization or rule that underlies business policies.

Policy – A high level statement of an organization’s requirements around security, privacy and other business related practices and procedures which generally define how a policy is to be implemented.

Stakeholder Groups	
1. Clinicians (including physicians, nurses, mental health professionals, etc.)	10. Medical and public health schools that undertake research
2. Long term care facilities and nursing homes	11. Public health agencies
3. Physician groups	12. Quality improvement organizations
4. Homecare and hospice	13. Community clinics and health centers
5. Federal health facilities	14. Consumers or consumer organizations
6. Correctional facilities	15. Laboratories
7. Hospitals	16. State government
8. Professional associations and societies	17. Pharmacies
9. Payers	18. Regional Health Information Organization (RHIO) or Health Information Exchange Collaborative (HIE)
Domains	
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.	
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.	
3. Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.	
4. Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.	
5. Information protections so that electronic personal health information cannot be improperly modified.	
6. Information audits that record and monitors the activity of health information systems.	
7. Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.	
8. State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.	
9. Information use and disclosure policies that arise as health care entities share clinical health information electronically.	
Classification	
1. Barrier – Identified obstacles to the secure and private transmission of electronic health information. Barriers can be legal or business process related.	
2. Aid – Refers to how well a business practice and/or policy permits electronic health information exchange.	
3. Neutral – Neither a barrier or aid, neutral with respect to interoperability.	

8.4 Solutions Template

**Privacy and Security Project
Solutions Work Group Template**

Name of Solutions Work Group Member:
Please list the project number(s) of the business practice(s) addressed by the proposed solution (to be provided). The project number format is: RTI1_S2_D3_004.doc.

Please indicate the Stakeholder Group and Domain of the business practice you are addressing:			
Stakeholder Group:		Domain Addressed:	

Select a Solution Category:
<input type="checkbox"/> 1. Legislative <input type="checkbox"/> 2. Regulatory <input type="checkbox"/> 3. Technical <input type="checkbox"/> 4. Administrative or organizational policies and procedures <input type="checkbox"/> 5. Education

Please write in your solutions using the guiding criteria listed below:	
1. General context for the solution (what issues are being addresses with business practice or legal?):	
2. Proposed change/action (brief description):	
3. Benefits of proposal for health information exchange (brief description):	
4. Statutes/regulations affected (if applicable):	
5. Stakeholder(s) responsible for implementing solution:	
6. Stakeholder(s) responsible for funding solution:	

7. Stakeholder(s) impacted by proposed solution:	
8. Estimated costs to implement (brief description):	
9. Type of health info exchange affected (lab, clinical, research, etc):	
HIE Barriers addressed	
State of development of the solution (proposed, tested, etc.)	
Extent to which solution in use – by whom, how long, what areas of HIE?)	
Extent to which solution appropriate for a wide range of stakeholders and HIEs	
Possible barriers to solution	