Privacy and Security Solutions for Interoperable Health Information Exchange

Final Assessment of Variation and Analysis of Solutions Report

Subcontract No. 36-321-0209825
RTI Project No. 9825

Prepared by:

New York State Department of Health
Corning Tower
Empire State Plaza,
Albany, NY 12237

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

Submitted to RTI: March 30, 2007

RTI INTERNATIONAL

Table of Contents

Executive Summary

It has been said that the brick and mortar 20th Century health care delivery system will be replaced in the 21st Century with a health information and communications technology infrastructure that is accessible to all patients and providers. [Institute of Medicine, "To Err is Human: Building a Safer Health System," (Nov 1999).] Enabled with clinical decision support tools and powered by interoperable technology, this infrastructure offers the opportunity to improve the quality and efficiency of the care delivered while giving consumers better control over their health care experience.

Strong policies that protect the privacy and security of health information are crucial to achieving this transformation. Patients share a great deal of sensitive personal health information with their physicians and caregivers. This information is then shared with insurance companies, pharmacies, researchers, and government, for reasons such as treatment, payment, public health and research. Without adequate privacy protections, individuals take steps to shield themselves from harmful and intrusive uses of their health information, often at significant cost to their health. A consumer-oriented privacy and security framework that ensures personal health information is used in an appropriate and transparent matter is essential to earning the trust of patients and to the ultimate success of electronic health information exchange (HIE).

Current laws governing HIE and the resulting business practices were developed in the context of a paper world where decisions on what to communicate, how and to whom are generally made on a one-to-one basis by clinicians. The current laws attempt to serve the patient's privacy interests by restricting what can and cannot be shared and the terms on which sharing takes place. Human judgment and personal relationships play a major role, as clinicians attempt to act as the guardian of their patients' information. However, from the standpoint of the patient's health and wellness, the system falls short. Patients have difficulty accessing their own personal health information and ensuring its availability at the point of care.

Moving from a paper to an electronic health system changes the information sharing dynamic. An interoperable health system facilitates a many-to-many relationship, enabling different information technology systems and software applications to exchange data accurately, effectively, and consistently. This offers new opportunities for patient access to and control over their health care information, as well facilitating the safety, quality and efficiency of their care. However, it also demands new approaches for protecting patient privacy and security, including policies addressing the disclosure and use of health care information, and technologies that address patient identification, authentication, record location, identity management, and storage of special classes of information.

The following report examines the current laws and business practices related to privacy and security of health information in a paper-based world, and begins to explore their implications on the transition to electronic HIE.

1.0 Background and Purpose

1.1 Health IT Initiatives in New York State

New York State is engaged in a statewide strategy to promote improved quality and efficiency of health care delivery through the use of health information technology (IT) and health information exchange (HIE). The State has secured and made available significant financial resources to promote the adoption of health IT and the development of infrastructure that promotes HIE. In addition, the State has undertaken the development of public-private partnerships that provide strategic development and evaluation for emerging HIE projects.

The Health Care Efficiency and Affordability Law for New Yorkers (HEAL-NY) Capital Grant Program is a multi-phase, $1 billion initiative that is being implemented over four years to reconfigure the State's health care delivery system and improve health care quality and efficiency. Two of the four phases so far are dedicated to providing investments in regional health IT initiatives. In its first phase, HEAL-NY provided over $52 million to support the development of clinical information exchange projects, the creation of e-prescribing capabilities and the use of electronic health record (EHR) systems. Grants were awarded to twenty-six (26) regional health care networks across the State. A list of the awardees and a short description of their projects is included in the appendix of the *Interim Assessment of Variations Report*. HEAL-NY is now in its third phase and a Request for Grant Applications was issued on November 14, 2006. Its goal is to build the necessary infrastructure to support interoperable HIE projects around the State.

Through the Centers for Medicare and Medicaid Services-approved, five-year demonstration called the Federal-State Health Reform Partnership (F-SHRP), the federal government will invest up to $1.5 billion in New York State reform initiatives (subject to special terms and conditions) that promote cost savings and efficiency in health care delivery of Medicaid services. One of the primary goals of this demonstration is to provide funding for the expansion of health IT and HIE among health care stakeholders including the adoption of EHRs and e-prescribing systems, and creation and sustainability of regional health information organizations (RHIOs). In addition to funding, the State would like to foster public-private partnerships that provide strategic direction for and promote monitoring and evaluation of current health IT initiatives. A representative from the New York State Department of Health (NYSDOH) chaired the New York HIT Stakeholders Group Planning Committee, which was supported by the United Hospital Fund. That committee issued a final report in July 2006 and led directly to the creation of a private Not-for-Profit Corporation called New York e-Health Collaborative, Inc. (NYeC), which was given a $100,000 grant by the United Hospital Fund. NYeC has a strong interest in further developing the State's health IT infrastructure and promoting the interoperability of regional health IT networks.

The New York State Health Information Technology Evaluation Collaborative (HITEC) is a multi-institutional project formed to evaluate and develop evaluation instruments for HIE initiatives across the State, while integrating a variety of stakeholders, including providers, payers, employers, foundations, the federal government, RHIOs and vendors. HITEC provides participating RHIOs with standardized surveys and outcome measures; consults on study design and other research methods for evaluation and data analysis; and reports on each RHIO (with comparisons to other

non-identified RHIOs). HITEC's cross-RHIO evaluations will produce statistics, trends and findings suitable for regional and national dissemination.

Finally, New York State continues to pioneer Medicaid e-prescribing projects, disease and care management demonstrations, and pay-for-performance initiatives. Together, these State initiatives—and multiple private and local initiatives—have contributed to a watershed moment; New York's health care industry is poised for transformation. As with any change of this scale, however, many questions and challenges remain. HIE projects and individual stakeholders are scrambling to find workable solutions to the myriad implementation issues that must be addressed to support the electronic exchange of health care information. Many have called for State or federal guidance to ensure consistency across projects, avoid wasted effort due to "reinventing the wheel" and to lay the foundation for a statewide, and eventually, national health information network (NHIN). However, the HIE environment is rapidly evolving in New York, and the understanding of the key technical, business and legal issues related to privacy and security is in a state of rapid flux. In addition, consensus has yet to emerge about many of the highly sensitive public policy issues that are raised by the transition to electronic HIE, and a process to facilitate such a consensus has only begun to unfold.

1.2 Health Information Security and Privacy Collaboration

The Health Information Security and Privacy Collaboration (HISPC) afforded an opportunity to initiative a statewide dialogue about how to address the privacy and security requirements of an electronic HIE. New York is one of thirty-four (34) states and territories charged with bringing together a broad range of stakeholders to develop consensus-based solutions that support the privacy of patients while enabling the secure exchange of electronic health care information. The United States Department of Health and Human Services (HHS) contracted with Research Triangle Institute (RTI) to manage HISPC in cooperation with the National Governors Association. The Agency for Healthcare Research and Quality (AHRQ) and the Office of the National Coordinator (ONC) are closely partnering with HHS to provide leadership throughout the project. NYSDOH has been designated to lead New York's participation in HISPC. NYSDOH has partnered, via a subcontract, with Manatt, Phelps & Phillips and Columbia University (the Project Team, Appendix C) to accomplish the goals and deliverables of the grant.

The NYHISPC project is guided by a representative steering committee of health care business executives and statewide leaders, and a legal committee comprised of public and private attorneys specializing in health care privacy and security law. These committees work together with geographically diverse stakeholder workgroups to define current health information challenges and build consensus around the action steps for New York State.

The project includes four major phases over the course of ten months, culminating in two final reports to be completed by April 2007. The project tasks are:

1. Assess Variations in Business Practices and the Law Related to the Secure Exchange of Health Care Information
2. Develop Solutions to Support Secure Exchange of Health Care Information While Preserving Patient Privacy
3. Develop a Plan to Implement the Solutions

4. Finalize the Assessment, Analysis and Implementation Plans

1.3 Purpose and Scope of Report

The purpose of this report is to provide the findings from the first two phases of the NYHISPC project. The first phase of the project, the Variation Assessment Phase, was dedicated to assessing the variations in business practices and the law that present challenges to the secure exchange of health care information. This work utilized 18 simulation scenarios to catalogue practical approaches to exchanging health information and the complex web of legal requirements, business practices, clinical demands and policy guidelines in today's paper-based health information world. In the second phase of the project, the Solutions Phase, the project developed practical recommendations in law, business practices and policy for preserving privacy while enabling the secure exchange of electronic health information. The report includes the findings from the *Interim Assessment of Variations Report*, submitted to RTI on November 6, 2006, and the *Interim Analysis of Solutions Report* submitted January 16, 2007.

1.4 Report Limitations

This report provides an incremental contribution to New York's efforts to transition to widespread electronic HIE. Where possible, the report makes concrete recommendations regarding policies and practices to protect patient privacy and support the secure exchange of health information. The breadth of the project focus and the timeline for project deliverables limited the project team's ability to fully address the wide range of issues raised in the Variations stage of the project, to build broad consensus around proposed solutions, or to fully research implementation plans. This report provides recommendations, but it is not intended to offer definitive legal guidance and/or preclude the legality of alternative approaches. The project team has defined a longer-term process to continue the work of this project promoting consensus-based decision making among diverse and representative health IT stakeholders.

2.0 Assessment of Variations

The purpose of this section of the report is to summarize the findings from the Assessment Phase of the project, which identified variation in law, business practice and policy related to health information exchange in today's paper-based health care system. This assessment is designed to provide a foundational understanding of the issues that must be addressed in the transition to electronic HIE.

2.1 Methodology

The Project Team convened approximately 80 representative stakeholders (Variations Workgroup, Appendix D) over a two-day period in August 2006 to discuss 18 Simulation Scenarios developed by RTI. The scenarios provided context to determine current business practices and potential legal or policy drivers influencing HIE. The scenarios addressed the following issue areas:

- Treatment
- Payment
- RHIO
- Research
- Law Enforcement

- Pharmacy Drug Use/Benefit
- Health Care Operations/Marketing
- Public Health/Bio-terrorism
- Employee Health
- State Government Oversight

The data collected during the facilitated scenario sessions for each issue area are indexed, attributed to a stakeholder group and analyzed according to 1) the type of participating stakeholder organizations, 2) the relevant privacy and security domains, and 3) critical observations. These findings are described in section 2.2 below.

In addition, the legal committee conducted an analysis of twelve of the eighteen scenarios targeted because they raise significant State law issues. The analysis identifies relevant provisions of State law under each of nine privacy and security domains provided by RTI included in Appendix G for each of the twelve scenarios. The findings are compiled in a memorandum and are attached separately in Appendix H, "New York State Legal Analysis by Scenario." An overview of the legal and practice variation is found in Section 2.3, below.

Finally, section 2.4 provides a summary of the key findings from the Variation Assessment phase of the project.

2.2 Summary of Scenarios, Stakeholders, Domains, and Critical Observations

2.2.1 Treatment (Scenarios 1-4)

Scenarios

Scenario 1: ER

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.

Scenario 2: Substance Abuse Referral

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 relevant for medical diagnosis. The requested substance abuse information is being sent to the primary care provider. The primary care provider intends to refer the patient to a specialist and send all of his/her information including the substance abuse information received from the substance abuse treatment facility to the specialist.

Scenario 3: SNF

5:30pm Dr. X, a psychiatrist, arrives at the skilled nursing facility to evaluate his patient, recently discharged from the hospital psych unit to the nursing home. 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.

Upon entering the facility Dr. X seeks assistance in locating his patient, gaining entrance to the locked psych unit and accessing her electronic health record to review her 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.

Scenario 4: Cancer Screening
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.

Stakeholder Organizations

- Clinicians
- Community Clinics and Health Centers
- Correctional Facilities
- Homecare and Hospice
- Hospitals
- Long-Term Care Facilities/Nursing Homes
- Medical and public health schools that undertake research
- Payers
- Physician Groups
- Professional Associations and Societies
- Quality Improvement Organizations
- State Government

Privacy & Security Domains

- #1: User and Entity Authentication
- #2: Information Authorization and Access Controls
- #3: Patient & Provider Identification
- #4: Information Transmission Security or Exchange Protocols
- #5: Information Protection (against improper modification)
- #7: Administrative or Physical Security Safeguards
- #8: State Law Restrictions
- #9: Information Use & Disclosure Policies

Critical Observations

The patient care scenarios prompted discussion of a broad range of business practices dealing with release of health care information, record management and security issues. Business practices governing the release of information dominated much of the discussion. Unlike HIPAA, New York law demands patient consent before the release of most health care information for treatment, payment or health care operations. While oral or implied consent is legally permissible, most institutional stakeholders require written patient consent for the release of health information to another provider. This is often implemented in the form of a general, one-time

consent signed by all new patients. Small practices and individual providers are more likely to rely on implied consent in their day-to-day operations.

However, practical exceptions to this rule exist, often driven by the clinical needs of the patient. Organizations desire and routinely seek to obtain appropriate patient authorization for record exchange, but when balancing data disclosure with patient privacy, provider organizations hold patient care as their ultimate driver. When appropriate consent cannot be obtained after a good faith effort, organizations feel justified in proceeding without consent in order to better serve the patient's health. For example, one hospital said they would allow release of information if the patient was unable to consent and if the organization treating the patient sent a fax on letterhead stating that they were treating the patient. Another hospital said they would accept oral assurance from the requesting organization, but only if they knew and trusted the organization and had two people on the phone to witness the conversation. Often, these exceptions are viewed as falling within the legal construct of "implied consent."

Organizations recognize and uphold the additional protections that are required for sensitive data. Providers often use special release forms, sometimes provided or approved by regulatory agencies, for information related to substance abuse, mental health, HIV/AIDS and genetic testing. These practices are rooted in federal (substance abuse) and State (mental health, HIV/AIDS and genetic testing) law. Some organizations create separate, secure storage areas for records with mental health or genetic information, and many described more robust efforts to ensure authentication of requests (verifying signatures, contacting the patient directly, requesting photo identification or even requests for notarized signature) when sensitive information was at stake.

Some providers are concerned that the practice of segregating sensitive health information such as mental health and HIV may at times create a risk to patient safety and ultimately impact patient care. At the same time, others observed privacy protective activities in their patients – such as asking that sensitive information be omitted from their medical record or not using their insurance for services related to sensitive conditions – that illustrated the desire on the part of patients for a higher level of protection than current practice affords. Some stakeholders suggested that standardizing the security and privacy safeguards across many sensitive conditions (e.g. mental health, HIV/AIDS, genetic testing, alcohol and drug abuse) might, in fact, better ensure consistent privacy protection and enhance quality of care. State officials noted that a single consent form for all sensitive issues has been developed by the State, but is rarely used by providers.

New York law contains a general requirement that disclosures to third persons "shall be limited to that information necessary in light of the reason for disclosure." *New York Public Health Law § 18(6).* New York law also specifically addresses the scope of disclosures in limited circumstances, including disclosures related to HIV/AIDS, *New York Public Health Law § 2782* and mental health *New York Mental Hygiene Law §33.13.* These requirements exceed the HIPAA concept of "minimum necessary," which does not apply to release of information for treatment purposes. Many stakeholders described business practices aimed at ensuring that only the information needed by the requesting provider was transmitted. Providers filter information both to protect patient privacy and to avoid the cost and administrative burden of replicating extensive paper records. It is common for records administrators to ask a requesting entity why they need the information if the

request seems excessive or out of the norm of practice. For example, a homecare organization typically only seeks patient status, medications and treatment orders, while primary care physicians generally request full access to patient history. Most stakeholders agree that health plan administration should only be allowed access to limited data relevant to payment and particular quality of care measures, rather than the entire medical record.

Once information is received from another provider, most organizations incorporate it into their internal medical records. Some organizations limit the information included to information used in the course of treatment, while others incorporate the full range of information provided.

Large organizations typically manage the complex and often nuanced questions regarding who gets access to what information through the creation of centralized units charged with all decision-making regarding the release of health information. While these privacy offices maintain high levels of compliance, some also acknowledge that physicians are verbally exchanging information with other providers to further patient care, stating: “At the end of the day, physicians have to take care of their patients.”

Most organizations are currently using a mix of paper and electronics systems. Multiple types of electronic systems, not necessarily interoperable, commonly exist within one organization. Use of electronic systems raises additional security issues. Some stakeholders said that all professionals within the organization with access to their electronic record have access to all information within the record, and professionals are trained to access only the information necessary to complete their responsibilities. Some electronic health records (EHRs) in use by stakeholders’ flag or separately store sensitive information to ensure it is not inadvertently printed and forwarded without proper consent. Most allow access only to credentialed providers. When it comes to exchanging information, these electronic systems essentially revert to a paper-based world, scanning paper records from other providers into the system and printing out portions of the record in response to requests from other providers.

Although it is recognized that laws and regulations may vary in different states, New York organizations disclosing information across state lines follow New York laws and regulations. Providers requesting information across state lines rarely encounter the need to vary their day-to-day operations to comply with neighboring state laws and regulations.

2.2.2 Payment (Scenario 5)

Scenarios

Scenario 5: Payer Access to EHRs
X Health Payer (third party, disability insurance, employee assistance programs) provides health insurance coverage to many subscribers in the region the health care provider serves. As part of the insurance coverage, it is necessary for the health plan case managers to approve/authorize all inpatient encounters. This requires access to the patient health information (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 health care provider’s workforce members and medical staff members and their office staff.
X Health Payer is requesting access to the EHR for their accredited case management staff to approve/authorize inpatient encounters.

Stakeholder Organizations

- Clinicians
- Community Clinics and Health Centers
- Homecare and Hospice
- Hospitals
- Medical and Public Health Schools that Undertake Research
- Payers
- Physician Groups
- Professional Associations and Societies
- Quality Improvement Organizations
- State Government

Privacy & Security Domains

- #1: User and Entity Authentication
- #2: Information Authorization and Access Controls
- #7: Administrative or Physical Security Safeguards

Critical Observations

Again, business practices governing the release of information dominated much of the discussion, specifically with regard to consent and the scope of the information released. While HIPAA allows release of a patient's health information without authorization for the purposes of payment, New York law has a higher standard. Most providers comply with State law requirements by obtaining a general consent, however others seek more specific consent for the purposes of sharing health information with a payer. Payers routinely obtain consent for disclosures as part of the initial enrollment contract or subscriber's agreement. It is likely that general consent would be adequate even for information related to HIV/AIDS or mental health conditions, as both laws permit general consent for payment purposes.

A level of discomfort exists among providers over allowing payers to broadly access provider electronic health records (EHRs). Part of this discomfort has roots in law. Under HIPAA a covered entity must develop policies and procedures that reasonably limit its disclosures of, and requests for, protected health information for payment and health care operations to the minimum necessary. New York similarly limits the scope of disclosure to information necessary in light of the reason for disclosure. *New York Public Health Law § 18(6).* However, providers also convey concern that information could be used by payers to avoid payment for services or to gain leverage in rate negotiations.

2.2.3 RHIO (Scenario 6)

Scenarios

Scenario 6: RHIO

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.

Stakeholder Organizations

- Community Clinics and Health Centers
- Correctional Facilities
- Homecare and Hospice
- Hospitals

- Long-Term Care Facilities/Nursing Homes
- Professional Associations and Societies

Privacy & Security Domains
- #2: Information Authorization and Access Controls
- #9: Information Use & Disclosure Policies

Critical Observations
While many organizations are currently engaged in planning and early implementation of RHIOs, very few in the State are currently exchanging data. For this reason, few stakeholders were able to offer business practices in response to this scenario. Most stakeholders agreed, however, that the exchange of patient-identified health information between providers and a RHIO for quality monitoring purposes would require the affirmative consent of the patient, and that special consent would be necessary to include information related to any sensitive health needs. New York law lacks any specific regulatory guidance for RHIOs, leaving organizations to make judgment calls on a case-by-case basis, considering the nature and scope of such consent. It is likely that the consent would need to be carefully crafted to ensure that the patient understood the nature and scope of the release, as RHIO activities are beyond what most patients would anticipate when signing a general consent for release of health information for treatment and payment purposes.

2.2.4 Research (Scenario 7)

Scenarios

Scenario 7: ADD/ADHD Data
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.

Stakeholder Organizations
- Clinicians
- Homecare and Hospice
- Long-Term Care Facilities and Nursing Homes
- Pharmacies
- Physician Groups
- Public Health
- State Government

Privacy & Security Domains
- #2: Information Authorization and Access Controls
- #3: Patient & Provider Identification
- #8: State Law Restrictions
- #9: Information Use & Disclosure Policies

Critical Observations

Again, the primary business practices raised in response to the research scenario related to consent and release of health information.

In most circumstances, federal law will govern research conducted, as in this scenario, on patients of a health care organization. Under HIPAA, a covered entity may always use or disclose for research purposes health information which has been de-identified. *45 CFR 164.502(d) and 164.514(a)-(c)*. To use or disclose protected health information without patient authorization, a covered entity must receive IRB or Privacy Board approval, or fall within several limited exceptions. *45 CFR 164.512(i)(1)(i).* Finally, covered entities are permitted to disclose protected health information for research purposes when authorized by the participant. This is most often the case with research trials, like those described in this scenario. *45 CFR 164.508.*

In the rare instances when the law is applicable for research on human subjects, New York requires that each person participating in research consent in writing to the research. *N.Y. Public Health Law § 2442.* The basic information necessary to any consent for research includes a "fair explanation" of the "procedure to be followed, and their purposes, including identification of any procedures which are experimental." *N.Y. Public Health Law § 2441(5)(a)*. New York does not have any statutes or regulations that address the redisclosure of information obtained in connection with research in this context.

There is a general lack of understanding among many stakeholders regarding legal requirements related to consent for participation and release of data for research purposes. Typically, health care organizations rely upon Institutional Review Boards (IRBs) to ensure adequate consent is obtained for both participation and data sharing purposes. Stakeholders questioned whether IRBs could play an active role in the facilitation of research by RHIOs.

This scenario also prompted a discussion of business practices related to consent from minors. Typically, providers seek consent from the parent of a minor (defined in New York as under the age of 18). However, some providers also noted that if the release related to sensitive health information, particularly for HIV/AIDS or reproductive health issues, consent would be sought directly from a minor. This practice, rooted in State statute, allows minors to consent to certain kinds of sensitive care and limits access to records for such care to the person who authorized the care. *New York Public Health Law §§ 17, 2781, 2782.* Similarly, State statute allows minors over the age of 12 to object to disclosure of medical records to a parent and the provider to deny the request. *New York Public Health Law § 18(3)(3).*

2.2.5 Law Enforcement (Scenario 8)

Scenarios

Scenario 8: 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.

Stakeholder Organizations

- Community Clinics and Health Centers
- Correctional Facilities
- Homecare and Hospice
- Hospitals
- Long-Term Care Facilities and Nursing Homes
- Professional Associations and Societies

Privacy & Security Domains

- #2: Information Authorization and Access Controls
- #4: Information Transmission Security or Exchange Protocols
- #6: Information Audits that Record and Monitor Activity
- #7: Administrative or Physical Security Safeguards
- #9: Information Use & Disclosure Policies

Critical Observations

The main issues raised by this scenario related to the release of medical information to both law enforcement officials and parents.

Some providers indicated that release of medical information about an individual patient to law enforcement would not be permitted without a court order. Circumstances under which providers are required or allowed to share medical information with law enforcement under New York State law depend on the condition at issue and circumstances under which the information is gathered. In the case of breath, blood, urine or saliva tests for the purpose of determining the alcoholic and/or drug content of the blood and administered by or at the direction of a police officer, consent is deemed to have been given under New York law. *NYS Vehicle and Traffic Law § 1194*.

In general, providers will not release health information to the parents of a patient over 18 without the patient's consent. As in the previous scenario, providers also noted that when sensitive information is the subject of the disclosure, e.g. HIV/AIDS, sexually transmissible disease information, mental health information, etc., they seek patient permission before release for patients over 12 years of age. Some providers indicated that where the release is to parents, verbal consent from the patient would generally suffice.

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

Scenarios

Scenario 9: Formulary Alternative

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.

Scenario 10: Switching PBMs

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.

Stakeholder Organizations

- Clinicians
- Community Clinics and Health Centers
- Homecare and Hospice
- Hospitals
- Payers
- Pharmacies
- Professional Associations and Societies

Privacy & Security Domains

- #2: Information Authorization and Access Controls
- #6: Information Audits that Record and Monitor Activity
- #9: Information Use & Disclosure Policies

Critical Observations

Again, the business practices invoked by these scenarios centered on consent and scope of disclosure. Under the scenario involving changing PBMs, the stakeholders observed that patient consent would not be required for a self-insured employer to share patient-identified data with the PBM. HIPAA governs this situation since self-insured employers under ERISA are explicitly defined as a "covered entity." *45 C.F.R. § 160.103.* Under HIPAA, authorization is not required for disclosure for the purpose of treatment, payment or operations. The stakeholders generally believed the disclosure would be within the definition of "operations." The scope of this disclosure, however, would need to be the minimum necessary for the purpose.

In the next scenario, the stakeholders addressed the situation in which certain medications require prior authorization to approve payment for a patient's medication. Currently, prior authorization for these medications is generally negotiated through phone conversations between the physicians and PBMs. In this case, the patient requested that the mail-order pharmacy fill a prescription written by the patient's doctor. Stakeholders agreed that the patient had thus given implied consent for the pharmacy and doctor to speak directly about the prescription in question, satisfying consent requirements governing both doctors and pharmacies under New York law. Again, only the minimum necessary data is shared to approve treatment requests.

Some organizations felt that this negotiation could be very difficult or even impossible to accomplish through electronic information exchange because of the need for the doctor to engage the pharmacy representative in a discussion of the clinical merits of the prescription. Others believed that online solutions had potential to negotiate the transaction. For example, the treatment request could be entered into the system, a justification provided, and review and approval given by the PBM; the approval could be transferred to the pharmacy, and finally an email could be sent to the patient that the prescription had been approved.

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

Scenarios

Scenario 11: New Rehab Center

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.

Scenario 12: Newborn Marketing

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 health live births).

The Marketing Department has explained that they will use the PHI 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.

Stakeholder Organizations

- Clinicians
- Community Clinics and Health Centers
- Homecare and Hospice
- Hospitals
- Medical and Public Health Schools that Undertake Research
- Payers
- Pharmacies
- Professional Associations and Societies
- Quality Improvement Organizations
- State Government

Privacy & Security Domains

- #1: User and Entity Authentication
- #2: Information Authorization and Access Controls
- #4: Information Transmission Security or Exchange Protocols
- #6: Information Audits that Record and Monitor Activity
- #7: Administrative or Physical Security Safeguards
- #9: Information Use & Disclosure Policies

Critical Observations

Organizations felt they had strong policies to determine when they could and could not use patient information for education, outreach, marketing and fundraising, which situations required authorization, which did not, and which were not allowed under HIPAA. In general, use of data for outreach efforts to educate patients about services available within the organization are not considered disclosures under State law and fall within permissible use of data for "business operations" under HIPAA. Some organizations noted the importance of ensuring that such activities could not

inadvertently reveal personal health information. Organizations noted, for example, that HIPAA prohibits targeted outreach activities based on diagnosis or condition. Others described efforts to ensure their physicians used the “blind copy” or “bcc” function in mass email communications with their patients, rather than sending an email to a list with viewable addresses.

Hospitals and health systems note that fundraising activities to patients and former patients, such as appeals for a capital campaign, also are permissible under HIPAA and frequently are a part of organizational operations. Most recognized more restrictive conditions under which patient information may be sold to a company for marketing purposes. HIPAA requires patient consent to use data for marketing purposes with few exceptions, and covered entities may not sell lists of patients or enrollees to third parties (as is suggested in this scenario) without obtaining authorization from each person on the list. *45 CFR 164.501, 164.508(a)(3)*.

Many larger organizations noted that any use of patient information for education, outreach, fundraising or marketing activities had to reviewed and approved by the privacy officer. Many also provide training on use of patient information for non-treatment uses, such as to fundraising, marketing and outreach staff. Some organizations also reported processes that support opt-out requests, as well as ways to eliminate certain characteristics from contact lists (e.g., death lists). Organizations also report that they conduct regular audits of all access of patient records and have in place policies and procedures to enforce rules and punish violators.

2.2.8 Public Health/Bio-terrorism (Scenarios 13, 15-17)

Scenarios

Scenario 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.

Scenario 15: Public Health, TB Carrier

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.

Scenario 16: Public Health, 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 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.

Scenario 17: Public Health, 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 provider, and is sent there for the medical care, and is referred to a

hospital-affiliated drug treatment clinic for his addition 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.

Stakeholder Organizations

- Clinicians
- Community Clinics and Health Centers
- Hospice and Homecare
- Long-Term Care Facilities and Nursing Homes
- Medical and Public Health Schools that Undertake Research
- Payers
- Pharmacies
- Physician Groups
- Professional Associations and Societies
- Public Health Agencies
- Quality Improvement Organizations
- State Government

Privacy & Security Domains

- #1: User and Entity Authentication
- #2: Information Authorization and Access Controls
- #3: Patient & Provider Identification
- #7: Administrative or Physical Security Safeguards
- #9: Information Use & Disclosure Policies

Critical Observations

Organizations regularly comply with reporting requirements mandated by the State and county for public health monitoring and surveillance purposes, for example, for outbreaks of communicable diseases, births, newborn screening, deaths, and gunshot wounds. Much of this data is identifiable and submitted electronically, mandated by specific provisions in State law for a wide range of health care providers, and permits or requires the disclosure of information without patient consent. While, on rare occasion, de-identified and publicly released reporting data is patient identifiable (for example, where only one heart transplant procedure was performed in the county), stakeholders generally are confident in the security and integrity of public health reporting mechanisms and procedures.

Since 1998, the NYSDOH Internet based communications infrastructure has provided secure exchange of reporting, surveillance, statistical, and general information with its public health and health provider partners through the Health Provider Network (HPN). The HPN is a HIPAA compliant system that currently supports reporting and information interchange pertaining to vital records and registries, disease surveillance and response, and health facilities management. The HPN also is used by the State as its principal means for disseminating and gathering important and sensitive information and data regarding bioterrorism preparedness, surveillance and response. HPN user organizations include New York State, New York City, and county health departments; hospitals, nursing homes, laboratories, pharmacies; social service, physicians, managed care and various emergency service organizations.

2.2.9 Employee Health (Scenario 14)

Scenarios

Scenario 14: Employment, Return to Work
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.

Stakeholder Organizations

- Clinicians
- Community Clinics and Health Centers
- Homecare and Hospice
- Pharmacies
- Professional Associations and Societies

Privacy & Security Domains

- #2: Information Authorization and Access Controls
- #4: Information Transmission Security or Exchange Protocols
- #9: Information Use & Disclosure Policies

Critical Observations

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

2.2.10 State Government Oversight (Scenario 18)

Scenarios

Scenario 18: Health Oversight, Immunization & Lead Screening
The Governor's office has expressed concern about compliance with immunization and lead screening requirements among low-income children who do not receive consistent health care. The state agencies responsible for public health, child welfare and protective services, Medicaid services, and education are asked to share identifiable patient level health care data on an ongoing basis to determine if the children are getting the health care that they need. This is not part of a legislative mandate. The Governor in this state and those in the surrounding states have discussed sharing this information to determine if patients migrate between states for these services. Because of the complexity of the task, the Governor has asked each agency to provide these data to faculty at the state university medical campus who will design a system for integrating and analyzing the data. There is no existing contract with the State University for services of this nature.

Stakeholder Organizations

- Clinicians
- Community Clinics and Health Centers
- Hospice and Homecare

- Long-Term Care and Nursing Facilities
- Medical and Public Health Schools that Undertake Research
- Payers
- Physician Groups
- Professional Associations and Societies
- Public Health Agencies
- Quality Improvement Organizations
- State Government

Privacy & Security Domains

- #2: Information Authorization and Access Controls
- #8: State Law Restrictions

Critical Observations

This scenario raised issues related to sharing Medicaid data. State and federal law require that the Medicaid Program restrict the use or disclosure of information concerning applicants and recipients to purposes directly connected with the administration of the State Plan for Medicaid. Organizations wishing access to Medicaid data must file a "data exchange application" with the Medicaid Confidential Data Review Committee explaining how the project is directly connected with the administration of the State Plan for Medicaid. *42 U.S.C. § 1396a(a)(7); 42 C.F.R. Part 431, Subpart F; HCFA Regional Letter, No. 79-32, reprinted in CCH-ANNO, MED-GUIDE ¶ 13,850.30.* Some stakeholders believed it was unlikely that this process would permit the use of Medicaid data to support an intra-agency effort aimed at immunization and lead screening requirements.

Stakeholders' note that data to support such efforts also may reside in other publicly held sources, such as the New York Statewide Planning and Research Cooperative System (SPARCS). To access this data, researchers must submit an application to the NYSDOH Data Protection Review Board (DPRB) and a research protocol to the DOH IRB, agree to keep all personal information confidential and that final reports may contain only de-identified or aggregated data.

2.3 New York Law and Practice Variation

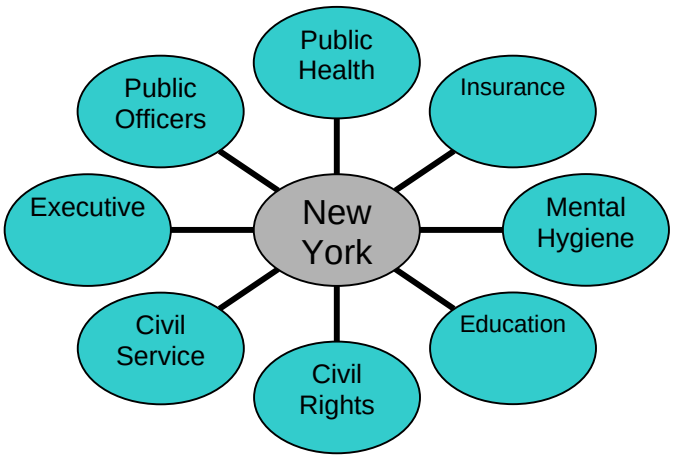
Unlike HIPAA, New York's extensive legal requirements governing the collection, storage and exchange of health information is not organized into a single regulatory scheme. State law governing health information is spread across dozens of statutory and regulatory provisions. The result is a patchwork of requirements and exceptions that vary greatly depending on the nature of the entity, type of information involved and purpose of the disclosure.

- *Nature of Entity.* Because many provisions of law governing health information fall under State licensure requirements, the type of entity exchanging information may determine what practices are appropriate or necessary. Fortunately, the law often imposes consistent requirements across several licensing schemes. For example, general consent requirements for disclosure of health information are the same for health care professionals, hospitals, nursing homes and pharmacies, though the law governing the various entities is scattered throughout the Public Health and Education Laws. However, this is not always the case.
- *Type of Information.* As discussed further below, special State law protections have been enacted to protect certain types of sensitive health care

information that could subject the patient to discrimination or embarrassment.

- *Purpose of Disclosure.* Finally, the purpose of the disclosure also may be relevant. For example, disclosures of HIV status without consent to a State agency for the purpose of public health surveillance may be mandated, where disclosure for law enforcement purposes would require a court order.

Exhibit 1: New York Statutes Governing Health Information Exchange (HIE)



New York laws governing security of HIE are general in nature and narrow in scope. As a result, compliance with the more extensive and detailed requirements under HIPAA generally ensure compliance under State law. For example, laws governing verification of treatment or coverage relationships, verification of requester's identity, transmission security, administrative safeguards, auditing and monitoring disclosures and information use, generally are either equally or less stringent or specific than requirements articulated in HIPAA. Failure to comply with HIPAA mandates may leave providers vulnerable to additional State sanctions. However, State rules generally do not necessitate business practices or procedures beyond those that would be required under HIPAA. However, this is not always the case.

Patient consent requirements in New York present the most common circumstance in which State law prompts variations in business practices for HIE. Unlike HIPAA, New York law requires consent for disclosures to third parties for treatment, payment or health care operations. General consent, often in the form of a one-time, broadly worded consent, is usually adequate for routine disclosures. While disclosures based on oral or implied consent are not explicitly prohibited by law, written consent provides a paper trail in the event of potential disputes and enables enforcement. As such, it is generally desired.

As in many states, however, general consent is insufficient in New York for certain protected categories of health care information. For example, a release of confidential HIV-related information must reference the nature of the information being disclosed, parties receiving the information and the purpose of the disclosure. This rule applies to all health care and social service entities exchanging information revealing HIV/AIDS status, though some exceptions apply where necessary for payment or treatment and in limited other circumstances. Genetic testing information also requires written consent, and the consent must specifically reference the fact that genetic testing results will be disclosed. Finally, mental health

information is subject to disclosure rules that result in special consent requirements. However, the restrictions only apply to information received from or held by facilities licensed by the State Office of Mental Health, Office of Alcoholism and Substance Abuse Services or the Office of Mental Retardation and Developmental Disabilities (OMH, OASAS and OMRDD, respectively), and some exceptions exist.

Other areas that are governed primarily by State law include the disclosure and use of information to and by public entities, including information gathered for public health monitoring and surveillance activities and disclosures for the purposes of law enforcement.

Across stakeholders, there are differing levels of understanding of and comfort with current legal and regulatory requirements. These differing interpretations translate into different business practices throughout the State. Organizations recognize the need for clarification and detailed education regarding current New York State and federal laws and their relative day-to-day application to health care treatment and operations.

2.4 Summary of Key Findings

The business practices that emerged from the scenarios represent the practical implementation of a complex web of legal requirements, business and clinical demands and policy goals. Common conclusions are drawn from the scenario discussions and legal variation analysis and provide a foundation for determining appropriate solutions. These conclusions are summarized below and described in detail in the following sections of the report.

- **Human Judgment in Information Exchange:** Information exchange currently relies heavily on human judgment and interaction to ensure security and privacy of health information.
- **From One-to-One to Many-to-Many:** Moving to a broad transfer of information to many persons or entities may require layers of sophisticated permissions and controls.
- **Informed Patient Consent:** Informed patient consent that is meaningful, tracked and monitored is a key requirement to earning patient trust in HIE.
- **Sensitive Data:** Differing regulations governing specially protected health information present challenges for staff education and compliance.
- **Appropriate Scope of Disclosure:** There is a need to more clearly define who needs to see what information and to understand how to accommodate appropriate access in an electronic environment.
- **Patient Care and Patient Privacy:** There exists a delicate balance between patient privacy and the need for information for treatment.
- **Security in an Electronic World:** There is a heightened sense of vulnerability regarding identifiable health care information in electronic form.
- **Use of Administrative Data for Clinical Purposes:** This practice poses an issue, since ideally, data should be gathered at the point of care for multi-purpose use. For example, the utility of billing data for clinical purposes should be reviewed.
- **Sharing Data Across State Lines:** Conflicting State laws create more complex challenges for those attempting communication among providers across State lines.
- **Support for Public Health and Syndromic Reporting:** Mandated reporting is achievable and there is support for public health collection of data.

- **Patient Control:** There is an opportunity to create an environment that supports the right of consumers to control the use of their own personal health information.
- **Role of Regional Health Information Organizations (RHIOs):** RHIOs can play an important role in HIE by acting as a trusted broker to establish and maintain privacy and security policies.

2.4.1 Human Judgment in Information Exchange

Human judgment plays a critical role in determining what information is shared and with whom in the existing day-to-day exchange of health information. While most stakeholders believe that patient records are exchanged with adequate authentication safeguards, most also acknowledge that the exchange often depends primarily on trusted relationships, intuition and judgment calls. Phone conversations between clinicians for purposes of treatment frequently replace the need for physically exchanged (paper or electronic) patient information. While providers and institutions are aware of consent requirements and generally build written consent into their business practices, they also say that the clinical and business demands of health care delivery sometimes necessitate diversion from these policies, often under the auspices of "implied consent." Authentication of requests for information is heavily reliant on relationships between organizations or individuals charged with information sharing.

2.4.2 From One-to-One to Many-to-Many

Moving from the current trusted person-to-person exchange to a system where information is accessed by potentially multiple unknown providers, payers or government entities will be difficult. Many stakeholders question whether patient information in an electronic information exchange can be as safe without the case-by-case judgment calls upon which paper-based health information exchange currently relies. Currently, both physical and procedural safeguards are in place to protect privacy and security and data is often exchanged in a controlled way with little delay and minimal paperwork through long-standing relationships that are "eye-to-eye" or one-to-one. There is general recognition of a need for systematic adaptation of current procedures for use in an electronic world. In an environment of ubiquitous electronic HIE, this personal or linear approach to data transfer must accommodate a broader transfer of information to many persons or entities who are unidentified at the time of loading the information into the HIE. Such an exchange may require layers of sophisticated permission and authorization controls.

2.4.3 Informed Patient Consent

It is recognized that *informed* patient consent is required to deliver all aspects of health care treatment and operations and that there is room for improvement to the health care system's current practices to obtain and maintain patient consent.

It is recognized that electronic systems must have the capability of tracking multiple levels of consent including, but not limited to, consent for treatment, payment, research and fundraising. Electronic systems also must have the necessary physical security safeguards in place to create a trusted environment. In situations in which providers use their best judgment to obtain consent for sharing information for treatment purposes, the protocols in EHR systems may be inadequate to re-create

the current mode of negotiation. Additionally, the concept of "implied consent," as opposed to the acquisition of written consent, may be impossible to accommodate in an electronic system. A requirement of a dated notation that consent has been obtained and by whom in the electronic record should be considered.

Finally, the State's lack of surrogate legal authority is generally recognized as a significant problem for determining consent in circumstances where the patient is unable to act on his or her own behalf.

2.4.4 Sensitive Data

Participants identified multiple "sensitive" health diagnoses that require additional levels of protection when compared to non-sensitive patient records. Mental health, HIV/AIDS, drug and alcohol abuse, genetic testing information, venereal disease and abortion records each require special handling or specific release authorizations. The differing regulations present challenges for staff education and compliance, and raise questions in an electronic environment. Some stakeholders suggested that a single, stringent standard to which all "sensitive diagnoses" or, in fact, all patient information could conform should be considered.

2.4.5 Appropriate Scope of Disclosure

Patients and providers alike are concerned about how to define who needs to see what, and how that might be accommodated in an electronic world. Exactly what patient information should be disclosed in situations of treatment, payment or operations currently is often negotiated between the requestor and the information source.

Considerable questions persist about how the scope of access can be adequately limited in a fully electronic world. This is one area where current practice often exceeds both State and federal requirements of law. EHRs often display the complete patient records, which support quality treatment practices but may compromise patient privacy. When all health providers have full access to patient records, patients perceive a lack of control over their own private health information. For example, the question was asked, "Why does my podiatrist have access to my mammogram?"

Stakeholders highlight that even with layered security in EHRs, parts of the record, such as clinical notes, often reveal diagnoses that may not be readily filtered, and flagging systems reveal by implication that a protected condition is indicated. In addition, as EHRs become broadly available, the systems must be able to accommodate the levels of security to adequately protect celebrity, VIP and employee records.

2.4.6 Patient Care and Patient Privacy

The balance between privacy protections and clinical treatment needs is a recurring issue encountered in each stakeholder's operations. Recognizing competing concerns and institutionalizing decisions about privacy and treatment needs is a key component of any successful EHR solution.

On one hand, there are extensive regulations that govern the storage and sharing of health information in an effort to protect patient privacy. On the other hand, best clinical practice often requires that providers have access to sensitive information in

a patient's record to make the most informed treatment decisions. While restricting physician views to only data that they need may be a solution, required information is difficult to predict at the case level. It may be impossible to systematically pre-determine what a clinician must access for optimum treatment.

Stakeholder organizations believe that patient education, informed consent, well-designed patient records and auditing controls can contribute to patient acceptance of electronic HIE. There also is desire for a common understanding or definition of "minimum necessary," as well as guidance for appropriate requests. Importantly, it is recognized that all disclosures must be tracked to adequately audit and enforce. However, questions remain about whether the scope of access by payers, employers, researchers and others may need to be more restricted. These questions reflect a heightened concern about the potential for misuse of information when the reason for disclosure is other than treatment.

2.4.7 Security in an Electronic World

Stakeholders are concerned about the heightened vulnerability of identifiable health care information in electronic, versus paper, form. Some stakeholders – including IT directors and RHIO participants – are concerned about the increased risks of data theft in an electronic system and the potential impact on patient trust and care.

2.4.8 Use of Administrative Data for Clinical Purposes

Currently, patient records are housed within multiple organizations. Some organizations may even have multiple records for a single patient. Currently, data submitted for payment purposes constitute the largest electronic databases available, providing a tempting starting point for early information exchange initiatives. Yet there is general agreement by stakeholders that such payment databases are not ideal for treatment purposes. Although they inform treating providers of some past medication history and diagnoses, payment databases are neither complete nor reliable. Further, providers often cannot access them on a timely basis, even if they are electronic, due to system failures, authentication difficulties and other challenges. As electronic exchange evolves towards a single record for each patient, it should create a system based on portable data gathered at the point of care. In the meantime, there should be common understanding around how best to accommodate for administrative data-set shortcomings.

2.4.9 Sharing Data Across State Lines

Stakeholders overwhelming said that sharing health information across state lines was rarely an issue in a paper-based world. Requests for information generally follow the home state procedures and laws of the party sharing the information. The requesting entity simply is expected to adapt. However, as regional exchange of health information goes to scale, conflicting state laws will create more complex challenges for those attempting to automate large-scale communication among providers across state lines. The human interaction – in which an out-of-state requester negotiates release – cannot be replicated in an electronic environment. And the increased flow of information will bring potential conflicts to scale – raising issues related to liability and jurisdiction for private stakeholders and government regulators.

2.4.10 Support for Public Health and Syndromic Reporting

Stakeholders support syndromic surveillance, which relies on health-related data that precede diagnosis and signal a sufficient probability of a case or an outbreak to warrant further public health response. Stakeholders agree that there is great opportunity in HIE to trigger early notifications based on diagnosis. Stakeholders acknowledge that mandated reporting to NYSDOH and local health departments is standard practice, and achievable on the existing electronic network.

2.4.11 Patient Control

Policy, law and consumer attitudes about the sharing of electronic health information have all developed in a world where most personal health information is collected, used, stored and disclosed by either health care providers who are treating a patient or health plan insurers who are responsible for paying for a patient's care. For the most part, laws restrict what can be shared and the terms on which sharing can take place.

With the emergence of electronic health information there is a significant opportunity to change the paradigm in which we think about who controls decisions regarding sharing and using health information. We have the chance to migrate from a provider/payer-centric perspective, where the emphasis is on restraining unauthorized use and disclosure of information, to a consumer-centric perspective where the emphasis is on empowering the consumer to have access to their own information and to be able to control who sees it for what purpose. In order to make this paradigm shift, states like New York must proactively create an environment that supports the right of consumers to control the use of their own personal health information.

2.4.12 Role of Regional Health Information Organization (RHIO)

RHIOs are emerging in New York, and across the nation, as a potential solution to implement community-wide HIE. One of the main functions of a RHIO – and driving force behind their emergence - is the potential for the RHIO to act as a trusted broker to establish, maintain and enforce privacy and security policies for multiple entities and for multiple purposes. Establishing a trusted broker for health information is not merely a matter of building a technical infrastructure that implements the dictates of State law and HIPAA. It requires developing a consensus around value-laden policy decisions, which are then translated into business procedures and eventually reflected in contractual relationships between RHIO participants.

One question that arises in the RHIO context is who owns patient data? Ultimately the answer to this question, whether it is the providers who create the data, the payers who fund the care, or the patients themselves, will impact a broad range of issues. Ownership of the data creates accountability for both the data's accuracy and its security; as well an obligation to protect the patient's privacy, ensuring that the minimum necessary information is shared with those with a right and a need to view the data. Ownership may also have implications regarding the funding of storage and exchange solutions. Ownership of the data may affect who can access and use the data, and for what purpose, and what authorization requirements are needed to share the data.

The success of RHIOs will depend on developing a clearer understanding of the range and scope of policy decisions, as well as a broader consensus of the principles that guide these decisions.

3.0 Analysis of Solutions

The second phase of the NYHISPC project offers solutions in the form of public policies, business practices, technical requirements and legal mandates that support the private and secure exchange of electronic health information to achieve the following objectives:

1. Facilitate consumers' access to their personal health information;
2. Provide treating health care providers complete and accurate information about patients in their care when and where they need it;
3. Ensure health care providers and other stakeholders have access to aggregated, de-identified and normalized patient health information for research, quality measurement and other quality improvement initiatives, including detecting and addressing quality variations; and
4. Enable health care providers and public health authorities to have timely access to information to survey and report communicable diseases, to address unsafe foods and medications, and to respond to disasters adequately in an efficient manner.

3.1 Methodology

In October 2006, a multi-representative Solutions Workgroup (SWG) (Appendix E) formed to review the challenges to secure and private HIE identified during the Variations phase. On November 2nd and 3rd the Statewide Work Group met to explore solutions to these challenges across multiple issue areas including Consent, Access/Authentication, Use, Security/Monitoring/Compliance, Patient Control, Simplification and Patient Identification. Each area generated numerous, diverse and at times even conflicting solutions, ranging from specific business practices and technology approaches, to broad public policy recommendations. The solutions generated were then reviewed by the steering and legal committees [Appendices A & B].

After reviewing the feedback from all workgroups, the project team [Appendix C] distilled the collected information into four main solution areas:

- **Patient Engagement:** Support the right of patients to expeditiously access their own clinical health information, and to make choices about the collection, storage, use and disclosure of their data; and engage people in taking a more informed and active role in their own health care.
- **Consent**: Ensure that patients are able to make meaningful consent decisions about the disclosure of their health care information, and that custodians of health care information comply with patient consent mandates under State and federal law.
- **Security / Access / Use:** Establish a common set of interoperable policies and technical requirements determining: (i) data access and use; (ii) authentication; and (iii) auditing, compliance and software and data security.
- **Patient Identification**: Provide for a reliable and secure method to correctly match patients with their health information, ensuring access to the right record(s) for the right patient at the point of care.

It is important to note that while public health reporting is a crucial component of planning and implementing HIE initiatives, during the numerous meetings and discussions with stakeholders, no one identified challenges related to reporting and disclosing personal health information to public health authorities as authorized or required by law and regulation. This is likely due to the fact that while privacy and security concerns are critically important in the public health arena, public health already has many solutions in practice. Compared with the newly emerging regional HIE projects, public health in many ways has a head start on securely exchanging, storing, and accessing confidential personal data. Thus, this report does not offer solutions directed to public health entities or public health reporting or monitoring activities. Further, this report does not suggest changes in existing public health mandates or authorized disclosures under State or local law.

In 2006, New York created the Office of Health e-Links New York within NYSDOH (Health e-Links Program) and appropriated $750,000 for the services and expenses of the Health e-Links Program. The proposed 2007 appropriations budget would provide another $750,000 for contractual services for the Health e-Links Program. The authorizing legislation requires that the Health e-Links Program be headed by a State Coordinator to enhance the adoption of an interoperable regional HIE. Thus, in the immediate future, the State Coordinator will have primary responsibility for implementing New York's solutions for interoperable HIE.

Each solution area is analyzed against a framework that offers four main implementation approaches:

- **State Coordinator and Advisory Body:** Appointment of a State Coordinator of the NYSDOH Health e-Links Program and establishment of a statewide, public-private group to convene stakeholders, make recommendations for aligning HIE policies, identify best practices for HIEs, provide technical, business practice guidance and recommend policies to the State Coordinator.
- **Accreditation Process:** Establishment of accreditation process for Health Information Exchanges (HIEs) that provide minimum standards for privacy and security solutions. A private entity could perform the accreditation but a State law would prohibit HIEs from operating unless they are accredited.
- **Clarification of Existing Laws and Regulations:** Call on the State government to provide guidance and clarification around existing laws that impact HIE to facilitate the smooth exchange of health information.
- **Promulgation of New Laws:** Develop new laws that address emerging issues in the transition to electronic HIE.

The interplay between the solutions that are described in this report and the implementation approach for each solution is illustrated in Exhibit 2.

Exhibit 2: Relationship Between Solutions and Implementation Approaches

Solution Areas and Implementation Approaches	State Coordinator and Advisory Body	Accreditation Process	Clarification of Existing Laws & Regulations	Promulgation of New Laws
Patient Engagement	X	X		X
Consent	X	X	X	X

Security/Access/Use	X	X	X	X
Patient Identification	X	X		

3.2 Analysis of State Proposed Solutions

The following section describes key challenges and solutions within each issue area (Patient Engagement, Consent, Security/Access/Use, and Patient Identification). The section is organized by issue area and includes for each a description of its objectives, a summary of the key challenges that were identified as priorities ripe for solutions, and one or more specific recommended solutions. The solutions were identified as priorities based on a combination of factors, including the urgency of the issue in implementing HIE projects currently underway in New York, and the degree to which consensus appeared to exist among project participants. The solutions themselves are organized according to implementation approach.

3.2.1 Patient Engagement

Objectives

1) Support the right of patients to expeditiously access their own clinical health information and to make choices about the collection, storage, use and disclosure of their data; and 2) engage people in taking a more informed and active role in their own health care.

Key Challenges

Although current federal and State laws mandate that people are given access to their health records held by providers and plans, the laws do not always establish a reasonable process for doing so. For example, medical records are scattered geographically, requiring many calls and letters of request. Since records are most often in paper form, they are expensive to maintain and copy (under current law, patients may be charged $.75 per page). Sometimes patients are unable to access their records at all due to the technical burdens presented by the duplication process. For instance, certain images (e.g. MRIs) often are not digitized and thus not easily duplicated.

The transition from paper records to electronic health information creates new opportunities to both enhance patients' access to information in their medical records, and to develop new ways for patients to maintain their own personal health information.

Even as we are rapidly developing health IT, nothing in the laws requires that people be given access to their records *in electronic form*. At present, most health IT initiatives are driven by the interests of providers and payers, because they are the current holders of medical records, without significant engagement of patient groups. In the absence of consumer-oriented constituencies, emphasis is rarely given to ensuring that patients have convenient electronic access to their own health data. As we transition to electronic exchange of health information, laws should be updated to provide patients the right to obtain health care information held electronically in an electronic format. These laws should address consumers' rights to access electronic information held by individual providers and payers, as well as information available through HIE projects.

Once personal health information is available in electronic format, consumers will be presented with more options for storing and maintaining it. Major efforts are underway by employers, health plans, private foundations and others to develop personal health records (PHRs) for individuals. While RHIOs and HIE initiatives typically seek to facilitate exchange of information between traditional custodians of health care information (providers and payers), PHRs can create opportunities for consumers to directly store and exchange their own health care information through third-party custodians. A wide range of entities could serve as third-party custodians under this model – including nonprofit organizations, private vendors or even RHIOs themselves. PHRs do not replace health records held by providers and payers, but exist in parallel for the patients' own use and convenience. Web-based solutions allow individuals to manage their PHRs online, and enable providers to transmit information to the consumer (and consumers to transmit to other providers) at minimal cost and inconvenience. The HIPAA privacy regulations and State laws govern some of these activities, but a company or organization that provides PHR services that is neither a HIPAA-covered entity nor a business associate of one may not be legally required to protect patient privacy.

PHRs hold great promise for making patient engagement more meaningful, but at this stage there is a dearth of clear and enforceable guidance on privacy and access policies in this arena. Without such protections, the market for PHRs held outside HIPAA-covered entities will be limited, due to legal uncertainty and consumers' privacy concerns. Opportunities to extend legal protections to third-party custodians under contract by consumers should be explored as another avenue for consumers to develop and maintain a personal health record.

Finally, in New York and around the nation, consumer and patient advocacy groups are skeptical about the potential benefits of creating health information networks—in fact, most of these groups are more focused on the potential negative consequences that can result from the misuse of their health data. A recent California HealthCare Foundation survey documents that half of the general population believe their health information is better protected in paper form. Out of fear that their sensitive health information will be used against them (i.e. loss of jobs, health benefits, stigma), a significant percentage of people avoid certain medical tests or treatment, withhold information from their health care providers, or ask providers to miscode a diagnosis or leave something sensitive out of the record. People with chronic illnesses and racial and ethnic minorities are even more likely to engage in these privacy protective behaviors for fear of discrimination. Further, consumers are not informed about the potential benefits e-health initiatives offer for access to care and heath care quality. There is a lack of awareness in the public and in the major consumer and patient advocacy groups that e-health can empower people to access their own records easily and inexpensively, and can make it possible for people to better manage their health (and the health of those they care for, such as an elderly relative or child).

There is a need for public education on the power of health information networks to identify and prevent medical errors, improve health care quality, tighten data security and limit breaches and other unauthorized uses of information. However, education alone will not earn public trust. Efforts must be made to engage more directly consumer representatives in policy and practice development concerning HIE, both at the statewide and project level.

Solutions

State Coordinator and Advisory Body

- Advisory Body advises NYSDOH with respect to a possible regulatory and policy framework for the development of PHRs, maintained by third parties, which are not covered by State or federal law.
- NYSDOH convenes, with assistance from the Advisory Body, a coalition or workgroup of consumer and health advocacy groups to provide input on a range of issues concerning HIE to ensure that consumers are informed and engaged at the earliest stages of the policy and design process, and that consumers' interests are considered at the outset, as well as to safeguard against potential backlash and criticism.
- NYSDOH, with assistance from the Advisory Body, develops public awareness campaigns, in coordination with consumer advocacy groups, to educate consumers on the benefits and risks of electronic health information and engage consumers to take a more active role in managing their own health.

Accreditation Process

- Create criteria for consumer engagement and participation in the governance and implementation of HIE projects.

Promulgation of New Laws

- Amend existing laws and policies to ensure patients have convenient and affordable access to their own health information in electronic format, where available, including, where appropriate, information available through HIE. This change should ensure that providers are adequately compensated for reasonable expenses related to the transfer of electronic health information, possibly through a combination of public resources and patient contributions, to avoid an unfunded mandate.
- Promulgate laws that protect the privacy and security of health care information held by third-party entities not covered under HIPAA who are acting as custodians of health care information on behalf of consumers.

3.2.2 Consent

Objectives

Ensure that patients are able to make meaningful consent decisions about the disclosure of their clinical health care information, and that custodians of health care information comply with patient consent mandates under State and federal law.

Key Challenges

Emerging HIE initiatives across the State are struggling to define what constitutes adequate and meaningful patient consent. Broad variation in opinion exists among stakeholders as to what is required legally, what is appropriate for risk management purposes, what constitutes the best public policy and what is feasible from an implementation perspective. For example, providers covered by the federal alcohol and substance abuse regulations may only disclose patient information to other providers if the other providers promise not to redisclose the information. How these various legal requirement and procedures are operationalized in an electronic environment is not yet clear. Nevertheless, some limited points of consensus exist.

First, HIE projects in general are structuring consent so that it is obtained and fully implemented at the provider level. The HIE entity may provide guidance on what standards should be applied for the purposes of loading and exchanging data through the HIE; however, the disclosing provider is ultimately responsible for obtaining and maintaining adequate consent. Second, it is clear that while consent is not necessary under HIPAA for treatment, payment or health care operations, under State law some form of consent is necessary to disclose patient information to persons or organizations external to the provider's legal entity, even for treatment purposes. The nature and degree of specificity required and the mechanism for obtaining consent to exchange health information is far less obvious, however. Third, stakeholders have different expectations and standards regarding consent when the exchange of health information is for purposes other than treatment. This is driven in large part by the belief that HIE for treatment purposes is more likely to be in the patients' interest and reflects the fact that the primary goal of HIE is to automate the transfer of patient records for treatment that currently occurs in the paper world. Because most HIE efforts in New York to date are limited to the exchange of information for treatment purposes, it is not clear how the standards differ when the purpose of the exchange includes payment, research or other purposes. (Note: Patient consent is not required for public health reporting and mandated disclosures under State and local law and, as such, those disclosures are outside the scope of this discussion.)

Beyond these broad outlines, diverse and often passionate opinions exist about what is legally required, what is best and what works—even within the steering and legal committees of the project. However, of prime importance is establishing credibility and trust vis-a-vis the patients and general public; otherwise, HIEs will fail as patients refuse to participate. With this in mind, three major options are discussed below.

General Consent. Some standard consent forms in use today may be adequate alone under the law for loading all patient information when the exchange is acting as an agent or contractor of the provider with a business associate agreement in place. Also, general consent is sufficient to exchange general health information among providers for treatment purposes.

Some have asserted that general consent is even adequate to allow the exchange of HIV/AIDS information, a class of specially protected information, among providers. This interpretation relies on an exemption within the HIV/AIDS special consent requirements for disclosures made when necessary for treatment. Others strongly disagree.

While simple to implement, using solely a general consent for the loading and exchange of information, raises concerns about meeting reasonable consumer expectations. In a paper-based world, providers are dependent on the patient to connect them to other providers serving the patient. In an electronic HIE, providers are given direct access to patient records, and information could be shared among treating providers without the specific knowledge of the patient. This paradigm shift, without specific notice, raises concerns that existing general consent forms might not constitute adequate informed consent by the patient. Not only could this expose providers to a higher risk of litigation, it could undermine patient confidence in the HIE, raising broader public policy implications. When extended to include sensitive health information, this concern and the risk of litigation is escalated considerably.

For these reasons, sole use of a general consent for loading and exchange of all types of information is not a recommended solution of this report.

General Consent, Plus Notice of HIE. An alternative approach is for each participating provider that previously has obtained a general consent to then provide each consumer with specific notice about the provider's intent to share the consumer's information within an electronic HIE, and provide the patient the option to choose not to participate in the exchange. Under this solution, the provider would have a general consent for the exchange of health information for treatment and payment purposes, as reportedly is now routinely obtained by most providers in New York State. In addition, providers would give written notice by mail or other reliable means to all patients. Such notice would inform patients that the provider intended to participate in an electronic HIE and, pursuant to the patient's previous consent, the patient's data would now be available electronically for treatment purposes to other participating providers. The notice could highlight the benefits of the data exchange to the patient in terms of convenience and care. Patients who did not want their information exchanged through the electronic HIE would have the option of notifying the provider in a reasonable and convenient manner within a reasonable time period and would be excluded from the interoperable exchange. Patient consent under this model could be driven at the provider level, so that patients could have the option of including health information held by one provider, while excluding information held by another. However, each provider would need to have the capacity to maintain records for non-participating patients outside the HIE.

This appears to be a reasonable approach for general health care information. However, it may not meet consumer expectations or legal requirements for specially protected information including HIV/AIDS and genetic information, and information from specially regulated mental health and substance abuse providers. While theoretically this data could be filtered or excluded from the exchange, this raises considerable technical challenges and serious clinical concerns, and risks denying the benefits of electronic HIE to the patients who arguably need it most. However, including specially protected data without the patient's understanding and support risks a serious breach of public trust and undermines the patient's ability to safeguard themselves against the potential misuse of such highly sensitive data. Thus, while this is a reasonable solution for general health care information, it is not a recommended solution for specially protected information, under either federal regulations for confidentiality of alcohol and drug abuse patient records or State law. Providers participating in HIEs utilizing this option either would need to screen such protected information out of the exchange, be otherwise authorized to receive such information (e.g. under the "necessary to provide appropriate care or treatment" exception to the HIV disclosure in PHL sec. 2782(1)(d)) or take additional action to safeguard specially protected information, such as seeking affirmative consent, as described in the third option below.

Specific Consent. A third option is to require that patients specifically consent to the sharing of information via the HIE. Consent could be obtained either at the point of loading information into the HIE (the "front end") or when treating providers seek access to the HIE (the "back end"). While this accords the highest degree of assurance of patients' consent due to the detail in the consent – it is more labor intensive. If consent is obtained prior to loading, some HIE projects fear that it is more difficult to populate the HIE with data. Projects starting with minimum data could fail, as providers, finding no information time after time, cease to access them. This concern can be mitigated by building patient consent into the early project

planning, so that by the time the system goes live, there is a critical mass of data. Alternatively, specific patient consent may be obtained at the point when a provider seeks to access the HIE. Under this approach, the HIE acts as an agent or contractor of the provider with a business associate agreement in place that allows the disclosing provider to load the information into the system. Once loaded, the HIE would release the information only upon receipt of appropriate patient consent by the patient of the requesting provider. To maximize patient control, the patient could authorize one provider to access the HIE, while refusing to consent for another provider to access the HIE. Thus, the patient could select some providers to utilize the HIE based on trust and perceived need for the information, while refusing to authorize other providers to access the information.

A major benefit of the specific consent approach is the ability to include, without question as to legal liability, specially protected health care information, including HIV/AIDS, mental health and substance abuse, and genetic testing information. This could be accomplished by developing a single consent document to cover all health information. NYSDOH currently has a single consent form in paper format that allows patients to check off boxes to disclose each specific type of sensitive health information, available but not mandated, for general use by providers. This form could be adapted to specify that the consent authorizes the sharing of all health information held by the provider, including specially protected information, in an electronic HIE.

While consensus has yet to coalesce around one of these options, there is an urgent need for guidance, as HIE projects and providers in New York are currently faced with creating the policies that will govern the consent within their projects. It is with this in mind that a hybrid solution, combining the second and third options, is offered. Under this hybrid solution, a general consent plus notice of the HIE would be adequate to exchange health information that is not specially protected, and a specific consent would be obtained to exchange specially protected health information. This specific consent could be obtained either prior to loading the information into the HIE or upon provider request for access to specially protected health information. Providers that did not obtain a specific consent at any point could access the information only if they were otherwise authorized by law to do so, e.g., in an emergency.

However, it is important to note that other options may exist and remain under consideration by State officials and stakeholder projects around the State. With all of these options, the operative consent may need to be durable until revoked. That is, the consent would need to be effective for repeated or ongoing disclosures, even for specifically protected information, unless a system were developed to allow consent to be obtained prior to each disclosure, like the system being developed by the New York State Medicaid Program in its Medicaid Medication History Pilot.

Solutions

State Coordinator and Advisory Body

- NYSDOH, with assistance from the Advisory Body, creates guidelines for obtaining meaningful consent for exchange of general and specially protected health information in the context of electronic HIE. Examine the feasibility of creating a single law specifically governing consent in the context of an electronic HIE.

Accreditation Process

- NYSDOH considers the recommendations of the Advisory Body to create consent criteria for HIE accreditation.

Clarification of Existing Laws and Regulations

- Issue policy guidance clarifying that general (not specially protected) medical information may be shared in an electronic HIE pursuant to a general release supplemented by notice giving patients ample opportunity to object to participation, where the HIE only discloses the health information to providers for the purpose of treatment.
- Develop a single form modeled on the current NYSDOH consent form, for use in obtaining consent, including for specially protected health care information (HIV, mental health, substance abuse, genetic testing, and venereal disease and abortion records) in an electronic HIE. Seek approval from the relevant State or federal agencies to ensure the form meets the approval of appropriate governing agencies.

Promulgation of New Laws

- If appropriate, create new laws governing electronic HIE and create legal safe harbors from liability for providers complying with the newly promulgated standards.
- Requires HIEs to be accredited.

3.2.3 Security/Access/Use

Objectives

Establish a common set of interoperable policies and technical requirements determining: (i) data access and use with respect to what types of data are accessible, who has access to which types of data, and for what uses or purposes; (ii) authentication with respect to how data is accessed securely by identified users and software applications; and (iii) auditing, compliance and software and data security, both at the point of care for treatment purposes and in the aggregate for quality and public health improvement purposes.

Key Challenges

As has been aptly pointed out by the Markle Foundation in its report entitled "Connecting for Health: The Common Framework," "the emergence of a networked electronic health information environment will transform patient care and improve the efficiency and effectiveness of the health care system. At the same time, the emerging electronic health information infrastructure and the massive increase in the volume of health data that is easily collected, linked and disseminated create unprecedented privacy and security risks that need to be adequately and appropriately addressed." (Connecting For Health Common Framework Model Privacy Policies and Procedures for Health Information Exchange, available at http://www.connectingforhealth.org/commonframework/docs/P2_Model_PrivPol.pdf)

Today, New York is ill-equipped to meet this challenge. There are no established public or private vehicles for considering, in the words of Connecting for Health, "the principles and policies that must be adopted to promote balance between consumer control of and access to health information and the operational need to ensure that information uses and disclosures are not overly restricted such that consumers would

be denied many of the benefits and improvements that information technology can bring to the health care system."

The issues that must be confronted go beyond developing a common understanding of what HIPAA or State law requires. Moving from a paper-based world which is heavily reliant on human judgment and one-to-one interactions, to a many-to-many world where information transfer can and will occur on a much more frequent basis requires determining over time new policies and standards with respect to data management, privacy and security policies and procedures. New York is investing significant dollars in the development and use of health IT and exchange capabilities, ahead of many other states in the nation. New York's challenge is how to put in place a policy and governance framework which allows investment and development to move forward while taking into account a range of factors, including new technology developments, emerging federal standards and policies with respect to HIE, and the need to coordinate, wherever possible, policy and technical plans of emerging information networks.

Specifically, it is critical that New York adopt a coordinated approach to addressing issues involving both policy and technical aspects of HIE with respect to (i) the security of health information and (ii) requirements relating to the access and use of health information.

With respect to the security of health information, it is critical that New York not duplicate existing efforts, but, instead, develop formal mechanisms for influencing and adopting emerging policies and standards that are developed through two federal public-private partnerships. These partnerships are the Health Information Technology Standards Panel (HITSP), which is charged with selecting standards to achieve interoperability through the nationwide health information network (NHIN), and the Certification Commission for Healthcare IT (CCHIT), which is charged with determining certification definitions and requirements for electronic health records (EHRs) and NHIN components, and inspecting products against the certification requirements. The task of influencing and incorporating the thinking of these two federally-sponsored initiatives should be the responsibility of the State Coordinator, with the advice of the Advisory Body. Once specific standards, policies and procedures are adopted, regional projects would be required to follow them through the accreditation process.

With respect to access and use of health information, the statewide Advisory Body should develop for consideration by NYSDOH a model set of policies and procedures governing the access and use of health information. Further, an accreditation process should be created to ensure HIEs adopt use and disclosure policies and procedures that meet an agreed upon minimum standard and put in place mechanisms to ensure their enforcement. It should be required that each HIE project adopt practices that ensure compliance with applicable federal, State or local laws and regulations, and with statewide policies and procedures covering use and disclosure of health information for health care delivery as well for law enforcement, disaster relief, research and public health. The data access and use policies and procedures should be set forward in a transparent manner and include agreed upon limitations with respect to the use and disclosure of information, including prohibiting accessing health information for marketing or marketing-related purposes, without specific patient consent.

Solutions

State Coordinator and Advisory Body

- Policy Interoperability -- Advisory Body Begins to:
  - Catalogue and assess existing data access and use, authentication and security policies among regional projects and HEAL-NY grantees as well as those from leading industry collaborations.
  - Determine a common set of data access and use, authentication and security policies by convening leading HEAL-NY HIE projects and national and State experts through a transparent and open process. Policies should address remedies for PHI breaches and data errors, appropriate role-based access rights, authentication and audit requirements, and comprehensive rules for secondary uses of health care data, including for research and the use of de-identified patient data.
  - Codify these policies for consideration by NYSDOH for standardized contractual and operational use among regional projects and HEAL-NY grantees.
  - Advise NYSDOH regarding the need for clarification of existing laws/regulations, and/or promulgation of new laws.

- Technical Interoperability
  - In order to avoid duplication of effort, NYSDOH will support the CCHIT in developing operational definitions for the technical requirements of the nationwide network components and inspecting them for their conformance with these definitions.
  - As appropriate for New York State purposes, NYSDOH will , with assistance from the Advisory Body, technical requirements and design for a statewide HIE broker as a component of HIEs and to interface to NHIN.

Accreditation Process

- Determine HIE accreditation criteria with respect to governance, organizational structure, and policy implementation and operations through an open, transparent process.
- Accredit HIEs as conveyers of public trust from a governance and policy perspective with respect to data security and encryption, authentication, access and use policies, and monitoring, auditing, and compliance processes.

Clarification of Existing Laws and Regulations

- Clarify laws governing access to Medicaid data.

Promulgation of New Laws

- Require that all health information sent to State agencies by a target year (for example, FY 2010) and beyond (including all health information exchanged within and between State agencies) conform to data standards and protocols established by federal Health Information Technology Standards Panel (HITSP) and incorporated by CCHIT where to do so does not compromise State and local public health activities and goals.
- Require State government to recognize HITSP and CCHIT standards in all relevant contracting, policies and programs to ensure adherence to a single set of HIE standards where to do so does not compromise State and local public health activities and goals.
- Requires HIEs to be accredited.

3.2.4 Patient Identification

Objective
Provide for a reliable and secure method to correctly match patients with their health information, ensuring access to the right record(s) for the right patient at the point of care.

Key Challenges
Stakeholders reached consensus around the importance of accurately matching patients to their records, and agreed more work should be done to develop a statewide solution. However, while there is a critical need for a workable solution, there is no consensus on a unified approach.

Debate continues at the State and national levels around creating a unique patient identifier and in New York, as nationally, the issue may be too politically contentious to offer a workable solution at this time. Establishing minimum necessary match criteria for patient ID—defining data elements that all exchanges in NY State could use—offers a practical alternative. Most notably, the Markle Foundation's Connecting for Health Program issued a prototype for patient authentication that involves an algorithm that may be equally secure and reliable—and less politically divisive—than a unique patient identifier.

Going forward, New York should make a concerted effort to study the options for patient identification, including their technical effectiveness and feasibility, cost and policy implications.

Solutions
State Coordinator and Advisory Body

- NYSDOH, with assistance from the Advisory Body, catalogues and assesses existing patient identification models implemented by HEAL-NY I grant funds and the National Health Information Network (NHIN) prototype contracts.
- Work with the CCHIT to develop certification criteria for the patient identification module of HIE or NHIN components.
- Explore pros and cons (including privacy concerns as well as the cost, benefit and value realization) of developing through a public-private initiative a statewide MPI. A potential testing ground for such an effort might be the creation of a statewide prescription and lab information exchange.

Accreditation Process
Require certified patient identification solutions as determined by CCHIT and supported by NY State assessment and pilot process.

3.3 Implementation Approach/Framework

As the Variations phase framed the problems to be solved, and the Solutions phase proposes ways to address those issues in HIE, the Implementation phase further explores approaches to put these solutions into practice. Many of the approaches cut across all the proposed solutions and seek to extend the work of this project beyond the life of the grant. Exhibit 3 illustrates the relationship between the specific solutions proposed and the implementation approaches. These approaches will be explored further in New York's final HISPC Implementation Report, to be submitted

in April 2007, which is written with input from the Implementation Workgroup (Appendix F)

Exhibit 3: Proposed Solutions and Implementation Approaches

Proposed Solutions and Implementation Approaches	State Coordinator and Advisory Body	Accreditation Process	Clarification of Existing Laws	Promulgation of New Laws
PATIENT ENGAGEMENT				
Explore creation of new laws/policies to protect health care information held by third-party custodians.	X			
If appropriate, promulgate laws for third-party custodians.				X
Create consumer coalition to engage consumers and protect their interests.	X			
Develop public awareness campaigns on the benefits and risks of electronic health information.	X			
Create criteria for consumer engagement and participation in the governance and implementation of HIE projects.		X		
Amend existing laws/policies to ensure patients have access to their health information in electronic format, where available.				X
CONSENT				
Clarify that general (not specially protected) medical information may be shared via electronic HIE for treatment purposes pursuant to a general release and notification.			X	
Develop a universal consent form that includes specially protected health care information for use in electronic HIE.			X	
Develop comprehensive guidelines and/or a single law for obtaining informed consent for electronic HIE.	X			
Create standards for certification taking into account the recommendations of the Advisory Body.		X		
Require HIEs to be accredited.				X
If appropriate, create new laws governing electronic HIE with legal safe harbors from liability for complying providers.				X
SECURITY / ACCESS / USE				
Ensure “policy interoperability.”	X			
Ensure “technical interoperability.”	X			
Determine HIE accreditation criteria through an open, transparent process.		X		
Accredit HIEs.		X		
Clarify laws governing access to Medicaid data.			X	
Require all health information sent to State agencies by a target year conform to federal Health Information Technology and Standards Panel (HITSP) data standards and protocols.				X
Require HIEs to be accredited.				X
Require State government to recognize HITSP and CCHIT standards in all relevant contracting, policies and programs.				X
PATIENT IDENTIFICATION				
Catalogue and assess existing patient identification models.	X			
Work with CCHIT to develop certification criteria based on pilot evaluation results.	X			
Explore pros and cons of a statewide MPI.	X			

Require certified patient identification solutions.		X		

4.0 National-Level Recommendations

The NY HISPC team has identified certain solutions that would benefit from being addressed at a national level, including:

- Model consent forms for loading information (routine and/or specially protected information) into a HIE.
- Model consent forms for disclosing Medicare information to and from a HIE (this would serve as a model for others).
- Clarify the applicability of 42 CFR Part 2 in connection with the inclusion of patient information regarding alcohol and drug use in a HIE.
    - Clarify for all states that a comprehensive consent to participate in a HIE encompassing various categories of protected information, without a separate check-off opportunity for alcohol and drug abuse patient records, is acceptable. A national model form created by the federal government will assist states and expedite the flow of information among states.
    - Consider an exception in the 42 CFR Part 2 regulations regarding that when a person gives his/her consent to disclose their information "to a provider for treatment purposes," this operates to disclose any and all information to a treating provider accessing the HIE—not only access to a subset of the patient's information which might be determined to be necessary to treat the particular condition/illness. Potential reconsideration by the federal government of the need for a prohibition on re-disclosure statements for each disclosure a HIE/provider makes in the context of a HIE. Possibly a single statement to this effect when a provider first signs on might be acceptable. The rationale being that if the statement is made routinely, no one will pay attention to it.
- Seek assurance that an electronic health record (EHR) which is released to an out-of-state provider receives the same high level of protection that exists if that electronic record were exchanged in New York. It appears to be the sentiment nationwide that consumers want to be given the choice to consent on a specific basis to the disclosure of sensitive medical information, even for purposes of treatment, as is required in New York. New York State expects that any national guidance on this topic will maintain New York's standard. New Yorkers would be reticent to share their information in an electronic exchange if the information would be subject to less protection.

5.0 Conclusions and Next Steps

In the final phase of NYHISPC, stakeholders explore the practical implications of the solutions recommendations and implementation framework. The objectives of the implementation stage are to determine who should take the lead in implementing each solution and approach; what resources are necessary to support these efforts; what the timeline should be for implementation; how activities underway at the federal level impact State initiatives; and how various efforts should be sequenced in light of limited resources and interdependencies of various efforts. These and other questions are addressed in the NYHISPC Final Implementation Report.

As this process moves forward, and New York continues on the path towards HIE adoption, it is likely that the new solutions will emerge, and recommendations made in this final report will continue to evolve. The NYHISPC Final Implementation Report aims to lay a path for continued work beyond the life of NYHISPC.

Appendices

Appendix A: Steering Committee

Dr. Gus Birkhead	Director, AIDS Inst. & Center for Community Health
Rick Cotton	VP & General Counsel, NBC Universal Inc.
Lisa Wickens	Asst. Director, Office of Health Systems Management
Tom Quinn	CEO, Community General Hospital
Dr. Philip Gioia	Medical Society of the State of New York (MSSNY)
Dr. Michael Caldwell	Commissioner of Health, Dutchess County
Wilfredo Lopez	General Counsel Emeritus and Consultant, New York City Dept. of Health & Mental Hygiene
Katie O'Neill	Senior VP & HIV/AIDS Projects Dir., Legal Action Center
Tom Buckley	CEO, Visiting Nurse Association of Albany
Dr. John Rugge	Hudson Headwaters Health Network
Harriet Pearson	VP Corporate Affairs & Chief Privacy Officer, IBM
Laray Brown	Senior VP, NYC Health & Hospitals
William Cromie	President & CEO, Capital District Physicians' Health Plan
Fred Cohen, Esq.	Senior VP and General Counsel, Independent Health
Bridget Gallagher	Senior VP, Jewish Home & Hospital Lifecare System

Appendix B: Legal Committee

Robert Belfort, JD	Manatt, Phelps & Phillips, LLP
William Bernstein, JD	Manatt, Phelps & Phillips, LLP
Deborah A. Brown, JD	Greater New York Hospital Association
Anna Colello, JD	New York State Department of Health
Melinda Dutton, JD	Manatt, Phelps & Phillips, LLP
Janlori Goldman, JD	Columbia College of Physicians & Surgeons
Jonathan Karmel, JD	New York State Department of Health
Wilfredo Lopez, JD	New York City Department of Health & Mental Hygiene (retired 12/22/06)
Anne Maltz, RN, JD	Herrick, Feinstein LLP
Donald Moy, JD	Medical Society of the State of New York
Katie O'Neill, JD	Legal Action Center
Jean Orzech Quarrier, JD	New York State Department of Health
Sarah D. Strum, JD	Catholic Health Care System
Robert N. Swidler, JD	Northeast Health

Appendix C: Project Team

New York State Department of Health

Jessica Kleinberg, Assistant Director, OSP	Contract Administrator
Bill Schroth, Chairman, NYS HIT Work Group	Project Director
Ellen Flink, Director of Research Patient Safety & Quality	Project Manager
Jean Quarrier, Associate Counsel	Team Member
Anna Colello, Director, Regulatory Affairs	Team Member
Jonathan Karmel, Associate Counsel	Team Member
Perry Smith, Director, Division of Epidemiology	Team Member
James Miller, Bioterrorism Epidemiology Coordinator	Team Member
Ivan Gotham, Director, HEALTHCOM Ntwk Sys Mgmt	Team Member
Theodore Hagelin, Director	Team Member
Robert Barnett, Director	Team Member
Debra Betor, Secretary	Project Support
Marilyn Soucy, Secretary	Project Support

Manatt, Phelps and Phillips

William Bernstein, Partner & Co-Chair, Government & Regulatory Division	Project Director
Melinda Dutton, Partner	Team Member

Manatt Health Solutions

Timathie Leslie, Managing Director	Project Manager
Susannah D'Oench, Consultant	Project Support

Columbia University

Janlori Goldman, Research Scholar	Project Director
Sydney Kinnear, Research Assistant	Project Support

Appendix D: Variations Workgroup

The following organizations participated in the HISPC statewide business practice variations workgroups.

ACOG
Albany Medical Center
Albany Memorial Hospital
Anheuser Busch
Association - Women's Medicine
At Home Care, Inc.
Bellevue Hospital
Bronx RHIO
Brownsville
Calvary Hospital
Cayuga Medical Center
Centrex Clinical Labs
Childrens Health Fund
Community Care Physicians
Community Health Center
Crystal Run Healthcare
Department of Corrections
Excellus Health Plan
Genesee Region Home Care & Hospice
Glens Falls Hospital
GNHYA
Greater Rochester RHIO
Greenberg Traurig LLC
Greene County Public Health
Harrison Center Outpatient
Health Care Providers
Health First
Hill Haven Nursing Home
Hometown Health Center
Hospital for Special Surgery
IBM
Institute for Urban Family Health
Interim Health Care
IPRO
Kings County Hospital
Kodak
Lab Alliance of Central New York
Lutheran Family Health
Memorial Sloan Kettering
Montefiore Medical Center
MSSNY
N. Shore LIJ Health System
Nathan Littauer Hospital
New York Presbyterian
New York University
Northeast Ortho
NY Health
NYC Health & Hospitals Corp.
NYC Health Plan
NYC Health/Hospitals Corporation
NYCLIX
NYHQ
NYS Association Healthcare Providers, Inc.
NYS Association of Health Systems
NYS Clinical Lab
NYS DoH AIDS Institute
NYSHFA
OMH
Prime Care
PSSNY
Queens Health Network
Revival Healthcare
Rochester Business Alliance
Saratoga Hospital
Seton Health Systems
St. Ann's Community
St. Peter's Hospital
St. Vincent's Manhattan
St. Vincent's Medical Center
Staten Island University Hospital
Stony Brook University
Stron Memorial Hospital
SUNY Stony Brook
Syracuse Chamber
UB Associates
United Health Services
Unlimited Care
Visiting Nurse Service of New York
VNA of Central New York
VNA of Hudson Valley
VNS/Signature Care
Westside Health Services

Appendix E: Solutions Workgroup

Abbondandolo, Donna	North Shore LIJ Health System
Angrignon, Rachel	Fidelis Care
Baig, Aleem	Metro Plus
Beato, Patricia	University of Rochester Medical Center
Blair, M.D., John	Taconic IPA, Inc.
Borges, Linda	MVP Health Care
Brucker, Julie	Saratoga Hospital
Burke, Donna	HealthNow
Calicchia, Eric Kate	Greenberg, Traurig
Chevalier, Lynn	Next Wave, Inc.
Cirillo, Joseph S. JD	Brooklyn Hospital Center
Clancy, Cathy	Hudson Health Plan
Cooper, Ellen	New York State Assoc of Ambulatory Surgical Centers
Ehlinger, Bryan	Oneida Healthcare Center
Ehrmentraut, Sheryl	Family Champions
Galanis, Christina	So. Tier Healthlink RHIO
Garnham, James	Greater Rochester IPA
Gillian, Paul	CDPHP
Groszewski, Walter	IBM
Heywood, Nancy	NYS Dept. of Correctional Services
Hoover, Robert	Independent Health
Iversen, Judy	Visiting Nurses
Iyer, Radhika	HealthNow
Jacomine, Douglas	CDPHP
Jaffe, Anita	MVP Health Plan
Julier, Kevin P.	IBM
Kelly, William P.	Treo Solutions
Kendall, Mat	DOHMH
Koch, Irene	Maimonides Medical
Kremer, Ted	Greater Rochester RHIO
Lurin, Joseph	GHI
MacMullen, Georgie	North Shore LIJ Health System
Majkowski, Ken	Rx Hub LLC
Martin, Donald	Fidelis Care
Martin, Dr. Glenn	Queens Health Network
Martucci, Joe	NYS Cyber Security & Critical Infrastructure Coor.
McCarthy, Kelley	So. Tier Healthlink RHIO
Meron, Stephanie	HealthNow
Murphy, Marie	Maimonides Medical
Novak, Carla	HANYS
O'Connor, Bill	HIP Health Plan
Pucherelli, Ron	MSSNY
Radin, Barbara	Bronx RHIO
Reed, Marian	McKesson Corp.
Reynolds, Cindy	NYHIMA & Hill Haven Nursing Home
Reynolds, Rita	Memorial Sloan Kettering
Richards, Cindy	HIXNY
Rudhika Iyer	HealthNow
Schirber, Mary Jane	
Shatzkin, Nance	BXRHIO
Silvious, Thomas	CSC Consulting
Taubner, Richard	HeatlhNow
Uhrig, Paul	SureScripts
Upadhyay, Asha	Taconic IPA, Inc.
Wendell, Matthew	MVP Health Care
Zink, Brian	CDPHP

Appendix F: Implementation Workgroup

Carol Allocco	Johnson & Johnson
Nick Augustinos	Cisco
Ellen Bagley	NYSHFA
Chris Baldwin	Northeast Health
Nancy Barhydt	New York State Department of Health
Patricia Beato	University of Rochester Medical Center
Maryam Behta	New York Presbyterian Hospital
Beverly Benno	Eden Park Health Care Center
Jo Berger	NYSDOH
Bill Birnbaum	Unlimited Care, Inc.
Erin Blakeborough	New York Association of Health Care Providers, Inc.
Rachel Block	United Hospital Fund
Maura Bluestone	Affinity Health Plan
Jim Botta	NYS DOH- Medicaid
Alan Boucher	Intel
Tammy Breault	Seton Health System
Deborah Brown	GNYHA
Julie Brucker	Saratoga Hospital
Thomas Buckley	VNA of Albany, Inc.
Michael Burgess	New York State Alliance for Retired Americans
Ann Burnett	NYSDOH - AIDS Institute & Uninsured Care Programs
Rachel Burwell	Cerebral Palsy of the North Country
Blair Butterfield	GE Healthcare
Thomas Carpenter	Affinity Health Plan
Diane Carroll	
Scott Casler	North Country Children's Clinic
John Cauvel	Lifetime Care
C. Lynn Chevalier	Next Wave Inc
Nicholas Christiano	Health Quest
Elizabeth Cole	Greene County Public Health Nursing Service
Ellen Cooper	Executive Woods Ambulatory Surgery Center
Rick Cotton	NBC Universal, Inc
William Cromie	CDPHP
Alice Cronin	Nyack Hospital
Liz Dears	Medical Society of the State of New York (MSSNY)
Linda Deyo	Greene County Public Health Nursing Service
Gregory Dobkins	NYSDOH
Maryann Dubai	Rome Memorial Hospital
Heather Duell	NYSDOH AIDS Institute
Kathleen Duffett	Kathleen Duffett, RN, JD, Attorney at Law
Kevin Dumes	Syracuse University
Craig Duncan	NYeC Board Member
Tom Ellerson	Lourdes Hospital
Simminate Ennever	Stony Brook University Medical Center
Lori Evans	Manatt Health Solutions
Donna Farago	Our Lady of Mercy Medical Center
Debra Feinberg	NYSCHP
James Figge	NYSDOH - Office of Health Insurance Programs
Carol Furchak	Crystal Run Healthcare
Christina Galanis	Southern Tier HealthLink
Beth Gallo	Waiting Room Solutions
Jim Garnham	GRIPA
Denise Giglio	Visiting Nurse Association of Utica and Oneida County, Inc.
Sharon Gonyeau	Cerebral Palsy of the North Country
Mary Hand	Glens Falls Hospital
Ken Harris	NYAHSA - The Center
Martin Hickey	Excellus BC/BS
Jeffrey Hirsch	Waiting Room Solutions
Susan Huntington	Glens Falls Hospital
Matthew Jarman	American Red Cross
Robin Jones	CMIp
Annette Kahler	Albany Law School
Mary Kenna	Group Health Incorporated

Brett Kessler	Bellevue Woman's Hospital
Al Kinel	Kodak
Irene Koch	Maimonides Medical Center
Susan Koppenhaver	Eden Park Health Care Center
Ted Kremer, MPH	Greater Rochester RHIO
Franklin Laufer	NYSDOH - AIDS Institute
Karen LeBlanc	Seton Health
Arthur Levin	Center for Medical Consumers
Liz Lonergan	Syracuse University College of Law
Joseph Lurin	Group Health Incorporated
Monica Mahaffey	Visiting Nurse Regional Health Care System of Brooklyn
Anthony Mancuso	Maimonides Medcial Center
Glenn Martin	Queens Health Network
Aileen Martin	North Country Children's Clinic
Roberto Martinez, MD	CDPHP
Joseph Martucci	NYS Office of Cyber Security
Mary Ann McGriel	Castle Senior Living at Forest Hills
David McNally	AARP
John Mills	HIP Health Plan
George Mina, Jr.	Canton-Potsdam Hospital
Lanetta Moore	Phase:PiggyBack,Inc.
Farzad Mostashari	New York City Department of Health and Mental Hygiene
Betsy Mulvey	NYHPA
Debra Mussen	CVPH Medical Center
Cynthia Nappa	SUNY Upstate Medical University
Carla Novak	Healthcare Association of NYS
Jeong Oh	Syracuse University
Renee Olmsted	Oneida Healthcare Center
Katie O'Neill	Legal Action Center
Michael Oppenheim	North Shore LIJ Health System
Johannes Peeters	Tioga County Health Department
Joe Phillips	Aurelia Osborn Fox Memorial Hospital
Scott Pidgeon	Palladia, Inc.
Ron Pucherelli	Medical Society of the State of New York (MSSNY)
Barbara Radin	The Bronx RHIO
Laurie Radler	Montefiore Medical Center
Carol Raphael	Visiting Nurse Service of New York
Rita Reynolds	Memorial Hospital
Cindy Richards	Northeast Health
Salvatore Russo	NYC Health & Hospitals Corporation
John Shaw	Next Wave Inc.
Ben Smith	Greater Rochester IPA
Robin Smith	ARCHIE:Adirondack Regional Community Health Information Exchange
Joseph Sorrenti	Interfaith Medical Center
Keith Stack	Alcoholism and Substance Abuse Providers of NYS
Susan Stuard	New York Presbyterian Hospital
Zebulon Taintor	Medical Society of the State of New York (MSSNY)
Deborah Tokos	United Health Services
Asha Upadhyay	THINC RHIO, Inc.
Teresa Yennan	Baptist Health
Daniel Walden	Medco Health Solutions
Mary Welch	Trudeau Health Systems
Robert Westlake, Jr MD	NY Chapter, American College of Physicians
John White	Our Lady Of Lourdes Hospital
Dianne Wilson	American Red Cross, New York-Penn Region
Lynn-Marie Wozniak	Next Wave

Appendix G: RTI Privacy and Security Domains

1) **Authentication of Identity:** 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) **Authorizations for Access:** Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

3) **Patient and Provider Identification:** Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.

4) **Transmission Security:** Information transmission security or exchange protocols (encryption, etc.) for information that is being exchanged over an electronic communications network.

5) **Data Integrity:** Information protections so that ePHI cannot be improperly altered.

6) **Audits and Monitoring:** Information audits that record and monitor the activity of health information systems.

7) **Administrative and Physical Security:** Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

8) **State Laws:** State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

9) **Use and Disclosure Policies:** Information use and disclosure policies that arise as health care entities share clinical health information electronically.