State of New Jersey
DEPARTMENT OF BANKING AND INSURANCE
CONSUMER PROTECTION SERVICES
PO BOX 329
TRENTON, NJ 08625-0329

JON S. CORZINE
Governor

TEL (609) 292-5316
FAX (609) 292-7522

STEVEN M. GOLDMAN
Commissioner

Privacy and Security Solutions for Interoperable Health Information Exchange

INTERIM ASSESSMENT OF VARIATIONS REPORT

Subcontract No. RTI Project No. 9825

Prepared by:
William J. O'Byrne
Sue Miller
Dorothy Gaboda
Amy Tiedemann
Deborah Cieslik
Sharon Joyce
Lisa King
Clifton Day
NJ-HISPC
New Jersey Department of Banking and Insurance
20 West State Street
P.O. Box 325
Trenton, New Jersey 08625-0325

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

November 6, 2006

Table of Contents

Executive Summary

This interim report is submitted by the NJ-HISPC Variation Working Group (VWG) and project leadership group to the Research Triangle Institute, Inc. (RTI) pursuant to Health Care Research and Quality Contract 290-05-0015.

The objective of this contract is to assess how privacy and security laws and business practices affect the exchange of interoperable health information; to examine how privacy and security policies and business practices regarding electronic health information impact on the exchange of said information; to convene and work closely with a wide range of stakeholders in New Jersey; and, to develop an implementation plan to address organization-level business practices and state laws that affect the private and secure interoperable exchange of protected health information (PHI). From the outset, it noted that this document uses "PHI" as the critical concept to define the scope of information on which this study focuses. In NJ, the PHI concept is also linked to the NJ Information Practices Act and the scope of information subject to privacy and security protections by certain industry parties may actually be broader than the HIPAA federal use of the term "PHI."

This interim report describes the methodology used by NJ-HISPC to elicit stakeholder responses to 18 health information data exchange scenarios supplied by the contractor that are designed to identify barriers to the exchange of PHI. It describes the barriers identified by stakeholders and by a panel of twelve public and private sector attorneys convened by NJ-HISPC Legal Working Group (LWG). Each scenario was reviewed in light of one or more of the 9 security and privacy domains identified by the contractor. The consolidated findings of the VWG and the LWG will be the subject of the work of the Solutions Working Group (SWG), and will be reported by NJ-HISPC in a subsequent report to RTI.

NJ-HISPC identified hundreds of different stakeholders that represent a variety of providers, payers, government agencies and consumer groups. The NJ-HISPC VWG then selected an appropriate number of relevant subsets of the various stakeholder groups to measure, consider and react to the content of the scenarios and related domains. Individual interviews, group meetings and conference calls were conducted, each of which was documented and reported by the project team. About eighty people provided input through focus groups and interviews. Thereafter, the LWG conducted an independent review of the scenarios, the domains and the business practices identified during the stakeholder interviews.

The preliminary findings, expressed opinions and barriers are summarized below:

- In some instances some identified processes and procedures are deemed to be "appropriate controls" on the dissemination and exchange of PHI even though they create a barrier to the rapid exchange of medical information.
- In multi-state situations, discussions with a number of stakeholders disclosed uncertainty and confusion regarding the application of the appropriate state's law pertaining to the consent requirements for the release of PHI associated in treatment, payment and healthcare operations.

- In addition, after meetings with stakeholders, NJ-HISPC's core group has observed that HIPAA itself was sometimes misunderstood by stakeholders to require creation of a barrier when it does not.
- Many stakeholders disclosed difficulty and confusion with the application of and compliance with HIPAA's "minimum necessary use" test in real life circumstances.
- Many technical and infrastructure barriers to electronic interoperability were identified.
- Many providers expressed a high level of comfort and acceptance of the existing business practices pertaining to PHI data exchange, such as telephone consultation, faxed documents and paper records. They do not yet fully recognize the efficiencies, benefits and quality of care improvements that will flow from interoperability of electronic health records.
- Some providers expressed a lack of certainty that more automated electronic processes would present substantial savings in the delivery of medical care in relation to the cost of implementation. These providers have advised the NJ-HISPC project manager that they recognize the potential savings for payers, but they are skeptical about the return on investment for providers.
- Financial resources and staffing limitations available to providers are frequently cited as an impediment to interoperability.
- Stakeholders identified specific categories of highly personal and "sensitive" PHI such as Sexually Transmitted Diseases, AIDS/HIV, mental and emotional health information including psychotherapy notes, substance abuse and genetic testing data that create special challenges for state and federal law and practice and may require special situational rules for the exchange of this kind of PHI.

The NJ-HISPC Solutions Working Group (SWG) will begin the next phase of project work as described above using these preliminary findings and other barriers discovered in the VWG and the LWG.

1. Methodology Section

New Jersey is geographically small, but has the greatest population density and the highest per capita income of any state in the country. It has urban centers of significant poverty in close proximity to rural areas dedicated to farm use and horse breeding. It is the home to many high tech industries and yet it has large areas of closed and rusting 19th and 20th century factories. Many of the 9/11 victims and their families were from New Jersey and it appears that the bio-terror/anthrax attack originated here. Given the great diversity found here, it was necessary for the NJ-HISPC to recruit working members and stakeholders from all areas in the state and from a broad range of backgrounds. The same mixture and composition found in New Jersey reflect many of the benefits, problems and challenges that are certain to exist to exist in the Country as a whole.

Consequently, the NJ-HISPC consulted with commenters from a wide array of divergent backgrounds in the completion of this phase of the project. The Variations Working Group (VWG) consisted of representatives from the New Jersey Department of Banking and Insurance, the New Jersey Department of Health and Senior Services, the Medical Society of New Jersey, the New Jersey Hospital Association, a network-affiliated hospital, an experienced nursing/home care consultant, and the Rutgers Center for State Health Policy. The VWG obtained information from commenters hailing from numerous organizations, facilities and activities to assure confidence that we had accumulated a variety of subject matter expertise to generate a complete and through itemization of business practices. The contributors included:

- Medical Society of New Jersey – primary care and specialty physicians, practice managers;
- New Jersey Hospital Association – physicians, information processing specialists;
- Hospitals – physicians, nurses, information processing specialists, mental health and substance abuse specialists, administrators;
- Payers – senior management, privacy officers, pharmacy benefit managers, information and IT processing specialists and claims managers;
- Home Care Association of New Jersey – staff and personnel from member agencies (nurses, care-givers and managers);
- NJ Department of Health and Senior Services – attorneys, public health officials, disease and mortality tracking, administrators of family-centered programs, bioterrorism experts, information security specialists;
- NJ Department of Human Services – Medicaid officials, mental health and family service officials;
- Nursing home and assisted living staff;
- New Jersey Manufacturers Insurance Companies – major domestic insurer with large book of business in auto insurance and workers compensation coverage.

- New Jersey Department of Military and Veterans Affairs – physicians, nurses, case managers;

- New Jersey Professional Boards – attorneys and staff, member physicians; and,

- Consumers and advocates for disabled children and adults.

Information was gathered from the stakeholders through a combination of focus groups and personal interviews. Members of the VWG met with and discussed the appropriate scenarios and developed a list of the applicable business practices suggested by the commenters. There was significant discussion on the nature, source and impact of the business practices identified. In some instances, the need for follow up information and questions was significant and further consultation with the commenters was conducted.

Because of delays in approval to convene the focus groups, NJ-HISPC and the VWG focused their initial efforts on personal interviews with sources identified in the proposal submitted by the NJ-HISPC. Thus, there was substantial contact and information gathered from: clinicians in several hospitals and in private practice; pharmacy benefit managers; mental health and substance abuse staff in specialty units; nursing home staff; information processing specialists; several state government agencies; and consumers. Many of the interviews were face-to-face, although in some cases contact was by telephone. These commenters provided the VWG with a significant initial list of business practices and provided a level of understanding of the variations in practice and policy.

Once approval was received to move forward with the focus groups, we held six focus groups around the state with state officials, hospital staff, the Department of Veterans Affairs, the New Jersey Home Care Association, and New Jersey Manufacturers. Each focus group lasted up to two hours and covered three to five scenarios. Business practices were identified and recorded from these activities. Subsequently, the VWG identified various areas where information was incomplete or unclear, and clarification was obtained through phone interviews or by email.

The NJ-HISPC and VWG reported the business practices in the provided RTI/AHRQ Assessment Tool throughout the data gathering process, and the information was available in the portal for review by VWG members. Also, the same information recorded in the Excel spreadsheet was distributed to VWG members and to our NGA and RTI representatives for review and comment.

The NJ-HISPC Legal Working Group (LWG) has commenced its work and includes attorneys from all aspects of the health care industry including: health care organizations, health care payers, the New Jersey Professional Boards, the New Jersey Department of Banking and Insurance, the New Jersey Department of Health and Senior Services, the New Jersey Department of Consumer Affairs, New Jersey Medicaid, the New Jersey Hospital Association, the Medical Society of New Jersey, the New Jersey Association of Health Plans, and several major law firms that specialize in privacy and security.

The LWG is reviewing the business practices collected by the VWG, and has formed into four study groups to review an assigned set of scenarios, domains and related business practices. The study groups have identified issues and relevant legislation and met by telephone and exchanged email to discuss their legal analysis of the practices. The results of these study group analyses

were provided to the co-chairs of the LWG and assembled into a template. The template is still being refined; and will be attached to the Interim Assessment of Variations Report. The full LWG will provide its analysis and identified additional issues now, and throughout the remainder of the project phases.

2. Summary of Relevant Findings Purposes for Information Exchange

2.1 Treatment (Scenarios 1–4)

2.1.1 Stakeholders

The NJ-HISPC VWG consulted with stakeholders from five different aspects of the health care industry to obtain information on the business practices that relate to PHI exchanges associated with the treatment of medical patients. (Scenarios 1 – 4)

Interviewed were:

1. Hospital Emergency Department and Marketing Department staff;
2. Clinicians practicing singly;
3. Clinicians in groups;
4. Substance abuse treatment facility staff; and
5. Nursing home and assisted living facility staff.

2.1.2 Domains

The NJ-HISPC VWG identified 33 business practices associated with the four treatment scenarios. These business practices impact on six different domains.

Nine of these business practices pertain to Domain number 9, Information Use and Disclosure Policies. These business practices include situations where the provider seeks to obtain patient consent to share PHI with other providers for treatment as well as the processes employed to give special protection to mental health and other sensitive PHI. In addition, the procedures for determining the nature and extent of what PHI will be shared with other providers were considered under this domain. As noted throughout LWG materials, there is no HIPAA requirement to obtain either consent or written authorization to allow for the use/disclosure of PHI for the treatment, payment and healthcare operations (TPO) purposes of the disclosing covered entity, or even for most disclosures for another covered entity's TPO. HIPAA allows these, except with respect to psychotherapy notes, without consent or authorization.

Domain number 4, Information Transmission Security or Exchange Protocols, was the next most commonly used domain classification, with eight of the treatment business practices falling within its scope. This includes cases where patients hand-carry their medical records between providers or where providers use dedicated secure web portals to transmit documents in an image or other document format.

Six of the business practices are covered under Domain number 2, Information Authorization and Access Controls. This includes situations where informal practices have developed between providers for sharing PHI and where more formal trading partner and/or business associate agreements exist. This includes cases where one provider can access another's medical records;

how the information is accessed when one provider uses electronic medical records and the other does not; and what information can be accessed by non-physician office staff.

The interviews placed eight business practices under Domains 1 and 8, User and Entity Authentication and State Law Restrictions. These business practices include using phone verification of provider identity; mechanisms to check the validity of a fax number; and specific state law restrictions on the sharing of HIV status and genetic information.

Finally, business practices associated with the location of fax machines for receiving and sending PHI and administrative processes that allow providers access to patient medical records from the provider's home are covered under Domain number 7, Administrative or Physical Security Safeguards.

The majority of the business practices cited in considering these four scenarios are coded as barriers to the interoperable exchange of health information. In each instance, the process of obtaining patient consent to share PHI with others introduces an interruption in the flow of information in both a paper environment and an electronic environment. Also, any steps taken to verify the identity of providers requesting patient health information add a delay to the passage of information in either a paper or electronic environment.

Lack of universal uniform standards for medical records add further delays in the movement of information in any systems. Thus, when providers have different types of medical records systems, such as paper and electronic, the transmission of information is complicated and steps are added to the workflow and processes. For example, having to both enter data into an electronic record and then print a hard copy disrupts the flow of information and the provision of medical care. It should be noted that delays associated with the inability to understand or access what is being reported simply because it is not in a universally accept format is an unnecessary waste of time and expense. Use of a consistent and accepted format, will ensure that all providers will have access to reported data. Consistency in format does not eliminate the delays associated with the encryption and authentication of identity issues but it can remove one easily rectified barrier.

Also, the VWG found various business practices based on state law and regulations restrict the sharing of PHI related to substance abuse, mental health and some specific diseases and make this information unavailable to other providers.

The Stakeholders outlined their understanding of several causes and/or reasons for the business practices applied or used within their organizations, including:

1. Internal organizational policies found in manuals, presented in training sessions or developed as a standard operating procedure,

2. Federal Law;

3. State Law, and

4. The practical reality and/or necessary to treat patients in emergency situations when time is of the essence.

Also, New Jersey statutory law may define certain conditions under which substance abuse information can be shared; this drives the practices of treatment facilities.

Or, in other instances, emergency department staff emphasized the exigent circumstances where patient care is their priority and necessitates the quick dissemination of critical PHI and has a practical impact on their health information exchange [HIE] practices.

2.1.3 Critical Observations

One issue of concern discovered in consideration of these business practices pertains to the different types of health information that providers were willing to share with other providers. There is not an agreed upon common data set of information that should be released to a requesting provider. There may be some regional practices agreed upon by the provider community which are driven by state law and local practice. While physicians will generally want all information in a patient's chart sent to another clinician, one exception is those clinics that treat substance abuse and mental health cases who will not freely share information. Also, there is no clear undertaking of the federal rules pertaining to what is included in the "minimum necessary" provisions.

Other variations in how entities share information relate to the differing information systems between providers, specifically the interface between electronic and non-electronic systems or lack of universal standards for EHR systems. Providers using electronic medical record (EMR) systems, often have two procedures in place for sharing PHI, one for sharing with others in the EMR network and one for entities that are not part of the system.

2.2 Payment (Scenario 5)

2.2.1 Stakeholders

For the Payment Scenario, the NJ-HISPC VWG interviewed payers handling individual health policies, employee group health plans, and disability insurance, plus hospitals, and home health care agencies. The perspective of home health care agencies was useful, since they also utilize case managers to coordinate patient care.

2.2.2 Domains

The NJ-HISPC VWG identified business practices for the following domains:

1. 1 – User and entity authentication;
2. 2 – Information authorization and access controls;
3. 4 – Information transmission security or exchange protocols; and
4. 8 – State law restrictions.

While different types of health coverage plans were discussed, business practices surrounding case management and approvals were similar. Where electronic exchanges occurred, user authentication was accomplished by requiring log-on identifiers and passwords for case managers and other authorized individuals to access the PHI in provider EHRs. Information authorization and access controls were outlined and defined in the business associate agreements between organizations. Information transmission security and exchange protocols included encrypted email and secure web portals for electronic transmissions as well as telephone contact

to assure that faxed information is going to the correct party. State law governs patient consent when an individual signs up for health care coverage. It should also be noted that specific HIPAA privacy exceptions permit payers' access to patient PHI when necessary for the payment of claims or as part of fraud detection and protection plans.

Barriers to interoperability include:

1. Difficulties of executing non-standard business agreements with a variety and number of payers;
2. Concerns with maintaining user access for individuals from many organizations without significant portal safeguards; and,
3. The comfort of many people with paper systems which they have used for years and a reluctance to experiment with unfamiliar technologies. This is a cultural barrier.

2.2.3 Critical Observations

1. Many providers still rely on paper systems to submit PHI to payers when seeking approval for medical services, procedures and referrals that require prior authorization; this notwithstanding, the payers have deployed systems for electronic transmission of this information.

2. Substantial resources are required to execute electronic trading partner agreements; to train individuals to use electronic data interchange of PHI; to deploy interoperable EHR formats; and, to maintain proper levels of privacy and security practices in a totally electronic environment.

3. Nonetheless, the commenters seem to recognize that the use of paper systems may also jeopardize the privacy and security of individual PHI, as several payers reported that there is always a great deal of uncertainty as to who actually sees a report when it is faxed, even if it is being sent to a previously verified fax transmission line.

2.3 RHIO (Scenario 6)

There is no NJ-HISPC report for this scenario as New Jersey does not have a RHIO.

2.3.1 Stakeholders

It should be noted that the NJ DOBI Task Force recently conducted a very successful conference on the new National Provider Identification Numbers. The Task Force used that opportunity to obtain the contact information on at least 200 stakeholders that have expressed an interest in working on projects associated with the creation of a RHIO and development of EHR in New Jersey.

On another front, several NJ stakeholders are in the process of organizing themselves together to develop a business plan for a self-sufficient RHIO.

2.3.2 Domains

Nothing reportable.

2.3.3 Critical Observations

There is a lot of interest in a RHIO in NJ and the NJ-HISPC core group plans to use this initiative as a launch point to bring the necessary parties together to take the next steps in developing a business plan for a self-sufficient RHIO.

2.4. Research (Scenario 7)

2.4.1 Stakeholders

For the research scenario, the NJ-HISPC VWG interviewed officials overseeing Institutional Review Boards [IRB] for human subjects' research at several universities in New Jersey. Also university websites were consulted pertaining to human subjects' research policies and practical applications. In addition, the VWG spoke with representatives of consumer advocacy groups as part of this endeavor.

2.4.2 Domains

The business practices associated with human subjects research fell into two domains:

1. Number 9, Information Use and Disclosure Policy and

2. Number 7, Administrative or Physical Security Safeguards.

Practices related to determining if the research activity warrants applying for a new project approval from the IRB, or filing an amendment to the existing project as well as the process of obtaining informed consent from study participants, are covered under number 9. One business practice for giving new researchers access to study data is covered under number 7.

Both the administrative process of applying for a human subjects' research project approval from a university IRB and the process of gaining consent from all necessary parties will interrupt the transmission of PHI and are coded as barriers. Approval of a research protocol can take up to a year at some institutions. Another barrier is the time involved when a Principal Investigator determines the level of access to be granted to other investigators in the use of the study data not to mention the time spent by a computing systems administrator applying the security and permission levels. The internal security for research data is handled within each project, often by informal methods; however, each Principal Investigator is responsible for protecting personal information. The federal Policy for the Protection of Human Subjects was the sole legal driver stakeholders mentioned as the reason for their university policies.

2.4.3 Critical Observations

Commenters reported that the length of time for approval of some protocols and the lack of standardization between entities can impact adversely on the product. While the VWG did not find variations in the actual business practices for this scenario, there are considerable differences in the length of the human subject project applications between institutions and how much documentation must be provided to the IRB for a project review. After applying, institutions also vary in the length of time it takes for investigators to be notified of approval or with requests for additional information. Administrative procedures to protect information

within a particular research project are not standardized, although they must meet the requirements of each institution's IRB.

2.5 Law Enforcement (Scenario 8)

2.5.1 Stakeholders

Regarding the Law Enforcement scenario, NJ-HISPC conferred with stakeholders from a hospital emergency department staff, physicians, and members of consumer groups.

2.5.2 Domains

The seven business practices related to sharing of information with law enforcement personnel fell into three different domains:

1. Number 9, Information Use and Disclosure Policy, contains processes for determining what information is given to the police officer present and what, if any, patient's rights exist to refuse the transfer of PHI to police authorities.

2. Number 1, Information Authorization and Access, and

3. Number 8, State Law Restrictions may limit the ways that hospitals can share PHI with parents when treating an adult child.

The patient consent requirements and procedures for determining what PHI goes to law enforcement and to parents prior to release are barriers to interoperability of health information.

The presence of a police officer and parents of an older child in the emergency department underscores the need for clinicians to understand state laws outlining the rights to health information and for legal purposes.

2.5.3 Critical Observations

1. The VWG found that hospitals handle the presence of parents of adult children patients in the emergency department in non-standard and different ways. One hospital's policy will permit discussion of test results with the adult child only; while another hospital's policy was to ask the patient's permission to give information to the parents.

2. Hospitals also reported a variance in how they decided what information to provide to law enforcement. One will leave it to the discretion of the attending physician while another only provides test results in suspected DUI cases and only when using police provided testing materials which are immediately returned to the officer.

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

2.6.1 Stakeholders

The NJ-HISPC VWG interviewed Pharmacy Benefit Managers (PBMs), employers, and physicians. They all provided information on the PBM scenarios.

2.6.2 Domains

The identified business practices for scenarios 9 and 10 fall into two domains:

1. Number 2 – Information authorization and access controls, and

2. Number 4 – Information transmission security or exchange protocols.

PBMs, their client companies, and physicians who use their electronic systems have business associate agreements in place that define who is allowed to view PHI and create systems of carefully construed increasing levels of access. There is also an adjudication procedure to process requests for exceptions, for certain high value and/or dangerous drugs, special reports and clinical information. Requests for prior authorization for drugs not covered on a formulary may be transmitted electronically or by paper, depending upon the system used by the prescribing physician. Even with an electronic system, an additional electronic form must be transmitted and approved according to the prescribed procedures, requiring business practices to assure the security of this transmission and access by only those individuals authorized to review exceptions.

PBMs may also be independently accredited for HIPAA and state law privacy and security compliance by national standard setting organizations that offer a greater degree of assurance to PBM customers that PHI is properly guarded.

Finally, PBMs will generally not use clearinghouses for the transmission of PHI that are not also similarly accredited as to privacy and security.

In some instances, payers are supplying physicians with electronic systems that employ encryption software to be used in conveying orders to PBMs in order to safeguard PHI. Where a physician uses a fax or email, they generally designate someone in their office to handle these secure transmissions. Requests from payers and others for special reports, such as a run of certain claims, are handled under written policies with adequate justification. When there are questions about the correct handling of a request for information, this is discussed with a company official responsible for privacy and security or the designated privacy officer. While some clients may request individual records for purposes of receiving competitive bids from PBMs, the PBMs themselves stated that they would request only aggregate information. Client companies may misunderstand what information is required as the “minimum necessary” (in compliance with HIPAA) and what privacy concerns exist for the personal health information of their employees. Transmission of electronic records to a client company is done through a

secure system such as VPN, email encryption, or a secure web portal. Encrypted records can also be transmitted physically on tape or CD-ROM.

Use of security procedures such as encryption and use of secure systems represent barriers to the exchange of information, but appear to be important for privacy and security of health information. Post-HIPAA, organizations seeking information to make competitive bids appear much more likely to request aggregate information rather than individual health records

2.6.3 Critical Observations

1. The determination of how to handle special requests from a client company may be more problematic in protecting PHI, since marketing representatives need to be sufficiently trained in HIPAA and other relevant legislation to know when to involve privacy and security experts in determining what information to release and the appropriate safeguards.

2. Encrypted electronic systems exist and are currently in use in the offices of primary care physicians to transmit routine electronic scripts to PBMs that are independently accredited as to privacy and security.

3. Scripts needing special processing or approvals are not generally handled within the systems described in item 2 above and, thus, PHI is exposed to a greater risk of potential compromise.

4. These encrypted electronic systems can be expanded to properly and adequately handle the adjudication process associated with the handling of special order scripts.

5. Fraud detection and prevention programs that reside in electronic systems provide a greater degree of efficiency and recovery than paper based systems.

2.7 Healthcare Operations/Marketing (Scenarios 11 and 12)

2.7.1 Stakeholders

The NJ-HISPC VWG identified eight business practices associated with the healthcare operations and marketing scenarios. This information was obtained from marketing and information technology departments in hospitals as well as from representatives of the home care industry.

2.7.2 Domains

The business practices relating to sharing of PHI for marketing purposes relate to three different domain categories:

1. Number 9, Information Use and Disclosure Policy, establishes policies that restrict what information can be used by hospitals for marketing and how it may be used. For example, several hospitals will share names and addresses of patients with internal marketing staff

only. None of the informants told the VWG that their entity would sell information to an outside firm.

2. Practices that authorize certain identified staff to work with PHI and to extract data for use by the marketing department are covered under domain number 2, Information Authorization and Access Controls. Most hospitals appear to have procedures in place to determine whether marketing activities are permissible under HIPAA, although not all hospitals would make the same decisions about marketing their services. Practices in home care agencies vary considerably, since these entities vary tremendously in size. Larger organizations have standardized policies and procedures to determine when data exchange is permissible for marketing purposes and to de-identify records as appropriate. However, respondents told the VWG that they believe smaller entities are much less likely to have standard practices for making decisions about appropriate handling of data for marketing purposes. Employees of these smaller organizations handle many functions and appropriate role definitions to protect the privacy of individual health information are less well established.

3. The way information is transmitted from one hospital department to another or to an outside entity, through encrypted email or shared networks files, is covered under domain number 4, Information Transmission Security or Exchange Protocols. Hospitals have written security protocols which are implemented by information technology staff.

All the business practices collected for these scenarios are coded as barriers. The processes for determining what data can be used for marketing, de-identifying data, and transmitting data securely, are clearly obstacles for the electronic exchange of health information.

2.7.3 Critical Observations

A major concern is whether these providers are willing to share names and addresses for marketing purposes. Home care agencies did not allow any sharing of demographic information for marketing, while hospitals allowed sharing of names and addresses internally, but only for the purpose of advertising hospital services. Neither home care agencies nor hospitals sold this information to outside companies.

2.8. Public Health/Bioterrorism (Scenario 13)

2.8.1 Stakeholders

Individuals from various New Jersey government departments provided information for this scenario, along with some individual physicians and hospital administrators. Many of the individuals who contributed had experience either with the actual anthrax incident in New Jersey or with various emergency preparedness planning and emergency drills. In some instances, these people dealt with the events of 9/11 and the aftermath.

2.8.2 Domains

Nine business practices were identified within the domains:

1. Number 2 – Information authorization and access controls;

2. Number 4 – Information transmission and security or exchange protocols; and

3. Number 8 – State law restrictions.

The VWG learned that most often medical information is transmitted by telephone, fax, or in person between local health agencies and the NJ Department of Health and Senior Services (DOHSS). DOHSS has responsibility for investigating and reporting communicable diseases and other related health and public safety incidents. Once it is clear that an anthrax incident (or similar event) is not isolated and is part of a possible bioterrorism event, the commenters believe that state and federal law allow sharing of information on a need to know basis with law enforcement, the governor's office, health providers, and first responders.

Business practices reflect the use of professional judgment in deciding how much information to communicate in each instance. For example, law enforcement needs to know sufficient information to conduct an investigation, and sharing of information needs to occur quickly and continuously. The Commissioner of DOHSS, as the chief protector of the public health, has broad public police powers to act to protect the general public, particularly once the Governor has declared a state of emergency. HIPAA provides no impediment to the appropriate disclosure of information to appropriate personnel in a state of emergency, both for actual treatment as well as general public safety/health reasons. However, it may be that "barriers" still exist, inasmuch as covered entities would still be required to take certain precautions in the exchange of information, such as verification/authentication of the recipient of data, proper safeguards in transmission of data, etc.

It is apparent from the interviews that barriers to the use of interoperable EHRs were more practical than legal, in the minds of our commenters. For example, police do not need or want to incorporate an electronic health record into their reporting about an incident. It is more useful for them to receive phone or fax updates about the location of incidents and the results of epidemiological investigation. Their interest in victims' medical information only focuses on those details that might lead them to a perpetrator(s) or source of the event. Information about the location of victims and the means of contracting anthrax (or similar event) are more important to them than details of any individual's electronic health record and the medical information contained therein.

2.8.3 Critical Observations

1. The major barriers for this scenario include state law and the security domains. Domain number 7, Administrative and Physical safeguards may be important in the future in defining controls that will assist in a number of the barriers in this area.

2. In terms of secure transmission of information by telephone and fax during a bioterrorism event, it is not clear that procedures exist to assure that protected information is seen only by authorized personnel. These issues are being addressed in bioterrorism preparedness planning in

hospitals and other settings, and will be explored more thoroughly by the Solutions Working Group.

An important issue about privacy that was related to the scenario arose: After the 9/11 attack, some hospitals in New Jersey were overwhelmed with calls from people trying to find their family members. Hospital staff mistakenly believed that they were not able to respond to these inquiries because of privacy rules. However, in future incidents, some hospitals have considered having a web site where the name of a patient could be entered and, if it matched an admitted patient, that information could be made available to the requester. However, no list of patients would be posted. It is not clear how such a system could or should be implemented in the future, but the ability to find relatives admitted to hospitals during an emergency is an important area of concern for the public. This may be a solution that works for a number of crisis situations but implications for privacy and security of personal information should be carefully considered by lawmakers and privacy experts.

3. In a state of emergency, assiduous enforcement and compliance with privacy and security laws, rules and directives are likely to be ignored in favor of the delivery of immediate and necessary medical care to members of the public.

2.9. Employee Health (Scenario 14)

2.9.1 Stakeholders

For this scenario, NJ-HISPC VWG obtained comments from hospital emergency room workers and employers. The VWG interviewed several employers suggested by the New Jersey Business and Industry Council, from very small to very large companies engaged in a wide variety of industries.

2.9.2 Domains

The business practices linked to this scenario are:

1. Number 2 – Information authorization and access controls;

2. Number 4 – Information transmission security and exchange protocols; and

3. Number 7 – Administrative or physical security safeguards.

The VWG determined that emergency rooms will not transmit PHI to any non-medical organization unless that institution has a business associate agreement with the requester. Employers do not expect to get information from the emergency room electronically. Generally, an employer's terms of employment or organizational policy requires that specific information about the employee's health problem be shared in two instances: 1) if the length of time the employee would be absent from work triggers a claim for temporary disability or workers compensation issue or 2) if the employee is performing direct care and needs to be certified as free of any communicable disease.

Transmission of the prescription form or letter from a doctor is usually by hand, mail, or fax. Employers reported that they stored medical information separate from their other employee records, in a locked filing cabinet in a secure location accessible to specifically assigned and authorized staff only.

Emergency rooms will not provide health information to employers without a business associate agreement due to their interpretation of HIPAA. Employers are less certain of what is required of them in processing and storing a return-to-work form, but some said their licensing agreements provided some guidelines.

2.9.3 Critical Observations

1. No procedures exist for employers to receive PHI from hospitals or physicians electronically and employers are not equipped to handle encrypted email. In most cases, they are not aware of the necessity to complete business associate agreements with all their business associates and do not know how to properly handle PHI.

2. It is not critical for employers to obtain PHI electronically.

3. Payers, including workers compensation insurers or third party administrators in the case of self-insured employers that handle claims for employers, should participate in the private and secure interoperable exchange of PHI with providers. The benefits of these electronic systems would clearly inure to the benefit of these stakeholders.

2.10. State Government Oversight (Scenarios 15–18)

2.10.1 Stakeholders

The NJ-HISPC VWG interviewed stakeholders from a variety of New Jersey state government agencies involved with:

- Public health, disease and mortality tracking;
- Professional boards that regulate the activities of health care providers;
- Payment of claims, regulation of payers, clearinghouses, third payer billers and third party administrators;
- Law enforcement;
- State university and institutions of higher learning;
- Delivery of assisted living and long term care to veterans; and
- Others involved in information security and oversight activities.

Also, information was also provided to the VWG by clinicians, law enforcement, and hospitals.

2.10.2 Domains

Identified were 25 Business practices in the domains:

1. Number 2 – Information transmission security and exchange protocols;
2. Number 3 – Patient and provider identification;
3. Number 4 – Information transmission and security or exchange protocols;
4. Number 8 – State law restrictions, and
5. Number 9 – Information use and disclosure policy.

Business practices of public health organizations revolved around the need to gather information required to track disease and protect public health, particularly in the scenario involving an active Tuberculosis carrier. In that case, New Jersey public health procedures prescribe cooperating with police to limit exposure by other members of the public, and disclosure of information to identify the individual with active Tuberculosis would be done by telephone to permit a rapid response. Providing information to another state to permit a public health response was also seen as protecting public health the by the stakeholder group. Information about all individuals involved would be solicited from the bus company, which is not a covered entity. All of the information exchanges are paper-based.

Business practices of hospitals and clinicians were driven by a concern for proper treatment of a patient and communication with patients. Physicians, hospitals, and laboratories tend to have business associate agreements in place that govern exchange of patient information. Physicians are interested in receiving all information necessary for effective treatment. However, disagreements exist about what information is necessary for effective treatment. Privacy considerations precluded disclosure of this medical information to relatives or shelters.

State government entities generally share PHI on a very limited basis; rather they gather information for disease registries and/or conduct investigations regarding compliance with state laws. Some limited sharing of information has occurred for the purpose of improving blood lead screening in children or other health information associated with public health issues.

Several types of barriers exist in the sharing of PHI for government oversight. Some are legal, such as the inability of Medicaid to share data about beneficiaries except for very limited purposes and the need to get parental consent to share information from disease registries. Others relate to the difficulties in accurately matching individuals across various databases, either because common identifiers do not exist or because of quality problems with the accuracy of identifiers. Public programs utilize a variety of enrollment and service encounter databases with different fields and formats, which are not easily merged. Even common identifiers may be used inconsistently; e.g. parents' social security numbers are sometimes used for children's records. Since data is often collected from many local/county enrollment sites, misspellings and duplications can compound inconsistencies which make accurate record merging difficult.

Agreements between a university or medical center and a state agency to share data are governed by business agreements which include paragraphs/appendices which specify data elements, if/when/how for disclosure of sensitive information, transmission, storage and retention of data.

Both types of entities also have Institutional Review Boards which protect the rights of human subjects in research.

2.10.3 Critical Observations

1. Restrictions exist regarding sharing of mental health and substance abuse treatment information. Physicians differed in how much of this information they would share with another provider. As outlined above, disagreements also existed over defining the minimum information required for effective treatment.

2. The significant difficulties in effectively merging data represent a daunting barrier to sharing of PHI. The cost of addressing this, along with restrictions governing sharing of information kept by the state in various departments and lack of current working relationships between state agencies are critical barriers to interoperability.

3. There are no procedures and/or programs for de-identifying PHI contained in electronic systems would permit rapid communicate of critical health information and alerts to the general public and to providers without compromising privacy and security.

4. Summary of Critical Observations and Key Issues

The NJ-HISPC, as a consequence of the hard work, wide ranging background and thoughtfulness of the focus groups and the variations working group, is able to submit the following interim summary of critical observations and key issues:

1. Stakeholders have established processes for sharing and protecting PHI.

2. Organizations that share PHI have rigid rules that focus the attention of their employees and agents on procedures and processes designed to protect the privacy and security of such information.

3. Most organizations tend to err on the side of caution in what PHI they will share and how they will share it.

4. In some instances, the application of privacy and security rules by organizations and their employees exceed the requirements of current laws and regulations.

5. There are differing opinions among stakeholders regarding what information is appropriate and necessary to share in response to a request for PHI from another health care provider. It appears that physicians define necessary information in the broadest way and desire that the most information possible be shared others while those involved in substance abuse and mental health facilities define necessary more narrowly and restrict the type information given to other providers.

6. When entities are sharing information with their own marketing departments, there is variation in the type and form of information that is made available.

7. There is uncertainty among providers and many others as when a signed consent is needed by a patient for the release of PHI. Many stakeholders believe that a patient's signature on a release is necessary even though the release may not be required by law for PHI exchanges related to treatment, payment, or health care operations.

8. Organizations encounter difficulties in HIE when the entities have different types of health information systems or structures. Unnecessary additional steps are taken when one entity is working electronically and the other is not; or, when non-compatible EHR systems are used.

9. There is a lack of connectivity between providers and between providers and others that should be involved in the exchange of PHI. Exchanges occur faster between providers in the same network or between entities that frequently work together. The majority of HIE transactions in New Jersey are still occurring using paper, phone, or fax machines.

4. Appendices

Appendix A - AT Data Collection Template.xls – posted on New Jersey portal under ‘Documents’

Appendix B – Legal Working Group Analysis.xls – posted on New Jersey portal under ‘Documents’