Privacy and Security Solutions for Interoperable Health Information Exchange

Interim Assessment of Variations Report

Subcontract No. 20-321-0209825
RTI Project No. 9825

Prepared by:

William D. Hayes, PhD
Health Policy Institute of Ohio
37 W. Broad Street, Suite 350
Columbus, Ohio 43215

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

HEALTH POLICY INSTITUTE OF OHIO

RTI INTERNATIONAL

Table of Contents

Executive Summary

In February 2006, Research Triangle Inc. (RTI) released a Request for Proposals titled the *Health Information Security and Privacy Collaboration (HISPC*) and invited the governors of each state to participate with a response. The Ohio Governor's Office asked the Health Policy Institute of Ohio (HPIO) to be the state designee for HISPC. HPIO, serving as a neutral trusted convener, has provided the leadership necessary for effective statewide collaboration and has a history of organizing statewide forums on critical health issues including Medicaid, obesity, health information technology, oral health and health disparities.

In May 2006, HPIO along with thirty-three states and one territory was notified that their proposal to represent Ohio on the HISPC initiative had been accepted. To complete the four tasks delineated by RTI, (1) Assessing variations in organizational level business policies and state laws, (2) Formulating interim solutions and an implementation plan, (3) Formulating final solutions and an implementation plan and (4) Managing the project, HPIO employed a broad inclusionary approach, empowering stakeholder participation in its processes, thus assuring an expansive scope in the review of interoperability, privacy and security issues. This report addresses Task 1: Assessing variations in organizational level business policies and state laws.

Task 1 involved the creation of several work groups to gather information and determine the legal implications of the issues identified by various stakeholders. The Variations Work Group (VWG) consisted of 15 members representing several stakeholder communities identified in the RFP. The VWG was charged with initial review of the patient privacy and security scenarios created by RTI and development of this *Interim Assessment of Variations Report.* To complete the assessment, comments on the scenarios were shared with the 25-member Legal Work Group (LWG). The LWG was responsible for identifying all issues that could represent a legal barrier to successful exchange of information. The VWG completed its initial review in early August and the LWG completed the legal review in late August. In addition, the project Ad Hoc Work Group (AWG) was also charged with filling the knowledge gap and providing expertise in areas where stakeholder input was limited. To further ensure a complete review of the scenarios, HPIO conducted a series of Topical Area Meetings (TAMs) focused on the specific needs of the individual stakeholders. Approximately 20 TAMs were conducted and the comments of the participants incorporated into the VWG review. HPIO was cautious about releasing information to the participants and only did so once the OMB release was obtained from AHRQ. A second round of reviews was then conducted by both the VWG and LWG and an invitation to comment was posted on the HPIO public wiki site. The wiki site (http://hispc.phwiki.com) was the primary tool used to communicate information and solicit input from the community at large.

The next step in the completion of this report involved entering the collective information into the RTI Assessment Tool. It was the responsibility of the VWG and LWG to enter the information in such a fashion that sorting and analysis could be easily facilitated. To that end, the groups arrived at the following naming convention State_Business Practice Number_Scenario_Business Practice Name. By using this convention the work groups were able to easily sort the information and simplify the process of compiling the records. Upon completion of the review, we identified approximately 200 business practices with corresponding policies and procedures. The majority of the business practices involved the authentication of a user, validation of information use, definition of minimum necessary, and fell into the domains of User and Entity Authentication; Information Authorization and Access; and State Law Restrictions.

Several significant findings were identified that must be addressed for this initiative to succeed. These findings include:

1. Establishing national standards for data exchange that must be adopted by all parties involved in the exchange of patient health information (PHI). The lack of any such standards coupled with the absence of an enforcement agency is the primary reasons for the failure to gain system interoperability across health care entities.

2. Creation of a universal patient identifier (or method) will also be a valuable tool in assisting data exchange and improving the security and privacy of the patient information.

3. It is our recommendation that the use of a role based system access model be standardized and implemented across the full spectrum of health care entities.

4. Funding, especially for rural communities, is a significant barrier to adoption of standards. As such, it is critical to have proactive financial support by the state government and/or through the development of public and private partnerships in Ohio. To that end, it will be most important for all stakeholders to be actively engaged in this effort.

5. Federal and state law requirements applicable to mental health and substance abuse records are stricter than the requirements of HIPAA.

6. The use of technology is viewed as a tool to improve systems interoperability with respect to privacy and security of information; however, it should not be implemented in the absence of a firm commitment to improving quality of care.

Each of these items represents a barrier to securing the patient record. The next step of this project requires that the Solutions Work Group (SWG) take these obstacles and create practical solutions designed to enhance quality outcomes, increase security of the patient information, and provide assurances that patient privacy will be secured.

Per the contract between HPIO and RTI, and consistent with our response to the Request for Proposal, this report and the processes followed for its completion has been reviewed and approved for submission by the Project Steering Committee.

1. Methodology Section

The Ohio Health Information Security and Privacy Collaboration (HISPC) project team employed a broad inclusionary approach to collecting the information used in the completion of this report. The intent was to empower the stakeholders in the process and ensure a comprehensive response to the issues of privacy and security.

There were three work groups principally employed in the development of this report and the second project deliverable. The groups included the Variations Work Group (VWG), Legal Work Group (LWG), and the Ad-Hoc Work Group (AWG). Each group was comprised of members from a broad range of health care backgrounds thus assuring an expansive review of the issues. For example, the VWG membership included health care information technology consultants, chief information officers (CIOs), security officers, physicians, attorneys, health plans, hospital administrators, state health associations and state government representatives. In total, the VWG has 15 members to represent the stakeholder communities associated with this initiative. Similarly, the LWG is comprised of 25 members, 23 of which are attorneys and 2 from other health care enterprises. Finally, the AWG consists of 49 members representing many stakeholder groups across the state of Ohio. The AWG was used throughout the project to supplement the information collection effort where representation on the VWG or LWG was lacking.

Each group conducted open meetings on a routinely scheduled basis. The method applied by the Ohio HISPC project team was to hold open discussions about health information exchange in the State of Ohio and surrounding states by inviting participation of all interested parties and by targeting specific stakeholder groups for participation. A consensus model process that used nominal group process to explore objections and to articulate areas requiring more granularity governs this “big tent” approach. This process provides the same type of consensus used by standards-developing organizations such as the American Society for Testing and Measurement. It streamlines discussion of the obvious, highlights distinctions and emphasizes the need to clearly articulate objections and nuances.

The process of information gathering required each group to first solicit input on the 18 scenarios from the group membership representing a particular stakeholder community. The VWG was the first to convene and review the scenarios. Initial feedback was provided to the LWG to ascertain if there were legal obstacles in Ohio that must be addressed before implementing any solution. The information was also provided to the AWG acting as an oversight committee and as supplemental staff to the VWG and LWG. Once the initial round of reviews was completed, the Ohio HISPC team, under the direction of William Hayes, President of HPIO, opened the dialogue to external stakeholders through a series of 20 Topical Area Meetings (TAMs). These meetings were open to the public and notice was posted on the project wiki site http://hispc.pbwiki.com. Specific stakeholder groups, such as pharmacy, long-term care, research, and rural health, provided the focus. Once the restriction for soliciting feedback from external stakeholders was lifted by the OMB, each participant in the Topical Area Meetings was asked to review the scenarios and post comments they might have through the wiki site. Those comments were forwarded to the VWG for a final review of the scenarios and the comments incorporated into this report.

Initial drafts of the report were provided to the work groups for comment. The *Interim Assessment of Variations Report* was then submitted to the project Steering Committee for final approval. Again, in the spirit of inclusiveness, each draft of the report was posted on the project wiki site with an invitation to external stakeholders to provide comment.

It is our opinion that broad based consensus, one of the primary goals for the Ohio HISPC project, was achieved. Because all meetings were open and publicly advertised, dissent could be voiced at any point in the process. Electronic communication and teleconferencing technologies were used to assure broad geographical representation in all discussions.

2. Summary of Relevant Findings Purposes for Information Exchange

2.1 Treatment (Scenarios 1–4)

2.1.1 Stakeholders: The principle stakeholders for the patient care scenarios include: Hospitals, Physician Groups, Clinicians, Pharmacies and Behavioral Health

2.1.2 Domains: The primary domains associated with these scenarios include: User and Entity Authentication and Information Authorization and Access. The relevant business practices include *Request to Release Information* when the request is coming from an entity outside of the treatment facility; *Assessing Patient Competence* where the treating physician must determine if the patient is competent to authorize treatment or if a person with a durable power of attorney for health care is the appropriate decision-maker. In either case, federal and Ohio law provides that if a patient is confused to the point that she cannot give consent, an adult relative does not have status in Ohio to provide consent unless the adult relative is the patient's guardian or is the named durable power of attorney for health care. Additionally, HIPAA 45 CFR 164.510 may be a temporary solution/exception that would allow the daughter to assist with decisions about the mother's health care.

The barriers that exist in these scenarios relate to authenticating the requested PHI and a lack of national standards pertaining to the exchange of information. Our experience indicates that the electronic medical record is an aid to health information exchange but must be standardized among disparate systems to be fully effective.

Additional business practices of note include scenario #2's S*ubstance Abuse Physician Referral* that covers a referral from a substance abuse facility to a primary care physician. Due to the Federal Drug and Alcohol Confidentiality Act (42 CFR Part 2), if the client's authorization cannot be obtained, a Qualified Service Organization/Business Associate Agreement must be entered into between the treatment facility and the primary care provider prior to disclosure. The primary care provider could not disclose records received from the substance abuse treatment facility to a specialist without the patient's authorization due to 42 CFR Part 2 and Ohio law's prohibition on re-disclosure (42 CFR § 2.32, OAC 3793:2-1-06(H). Also, *Patient Consent* used to release Personal Health Information (PHI) to an external entity, S*pecialist Referral* should the primary care physician deem it necessary to seek the assistance of a specialist, *Provider Identification* used to validate the caregiver has appropriate authority to view patient information, *User Access* to ensure access is restricted to only those with a legitimate need to view the information based on specific roles, *Validation of Business Associate Agreements,* should such support organizations be included in the treatment protocol, *Record Update* to provide protocols when exchanging information with an external entity, and finally the *Universal Precaution* clinical business practice for emphasizing awareness of conditions requiring unusual attention to prevent spread of infectious or contagious diseases. In that regard, the release of HIV information can only occur if the patient or patient's legal guardian specifically authorizes the

disclosure of information to the requesting party in the written release (ORC 3701.243).

2.1.3 Critical Observations: The reluctance to release (or re-release) PHI created by another entity is a pervasive problem based on a firm belief that it is prohibited. However, as long as HIPAA covered entities comply with privacy and security regulations, we are not aware of any legal basis for this position unless the information to be released pertains to mental health issues, drug and alcohol issues or research protocols. Thus it is a barrier, but not a legal barrier. There is no legal obstacle to obtaining information from a prior treating hospital when an emergency room physician needs it for diagnosis and treatment. According to the scenarios, the previous treating hospital may be in a neighboring state so there would be sharing across the state line. HIPAA clearly allows this as part of the treatment exception and there is nothing in Ohio law that would prevent this request for information. The neighboring state may want a signed consent form to send the information.

As noted in scenario #3, the behavioral health unit would need to ensure its physical access controls satisfy the HIPAA physical safeguards requirements, which could also help the unit satisfy Ohio law. Additionally, there is a key consideration, regarding access to mental health information between the HIPAA requirements that apply on a national level, and provisions of the Ohio mental health law, which are stricter. The HIPAA standards only apply to covered entities (and their business associates), and the regulations do not preempt more stringent provisions of state law. See ORC 5122.31

Regarding release of other PHI information created by another care provider, this may be a barrier, but again not a legal barrier. HIPAA applies to protected health information that the covered entity creates or maintains as health information. We are not aware of a legal cite for saying that an institution should only produce the information that it creates, so there may be no liability issues. We do know that most physician offices and hospital stakeholders have an internal policy that states they will only give information that they create. If they obtain test results from another site (physician office or IDTF) they tell the patient to get the information from the original site. We are not aware that this is a legal requirement. We have only seen it as an institutional policy. In regards to scenario #2, it is important to note that the Federal Drug and Alcohol Confidentiality Act (42 CFR Part 2), which pertains to substance abuse patient records, covers virtually all substance abuse treatment facilities and is much stricter than the requirements of HIPAA.

2.2 Payment (Scenario 5)

2.2.1 Stakeholders: The principle stakeholders for payment scenario 5 include: Payers, Consumers, State Government, Clinicians, and Hospitals

2.2.2 Domains: There are two primary domains identified for the payment scenario; Information Authorization and Access Controls, and Information Use and Disclosure. The first business practice identified by the stakeholders is *Payer User Access* for authenticating user need. Each stakeholder group has established differing procedures for authorizing access to patient information.

The methods used to satisfy this practice vary widely from telephone authorization to formal written request for access. Provided covered entities comply with existing statutes and regulations, this does not constitute a legal barrier. However, providing plan access through verbal authorization appears to have a high risk of unauthorized access based on a lack of documented authorization and may not satisfy the standard in 45 CFR 164.308. Health payers (other than workers' compensation) and health care providers are both covered entities as defined in CFR 45 106.103 and as such must comply with the minimum necessary standard set forth in 45 CFR 164.514(d). With regard to access levels, we have identified the *Minimum Necessary Information* business practice as critical to ensuring security and privacy of the electronic health record and further to provide that access is limited to the minimum necessary to satisfy the payers' needs. The flexibility of the minimum necessary standard itself creates interpretation challenges. This is an issue as it relates to privacy and security protocols.

2.2.3 Critical Observations: The single most significant and recurring obstacle in all 18 scenarios is a lack of standardized procedures for sharing information. This appears to be true for all aspects of Scenario 5. However, provided the covered entities comply with existing regulations, this obstacle is not a legal barrier. Covered entities are required to implement security standards, including technical safeguards to ensure the confidentiality and integrity of PHI transmitted electronically under 45 CFR 164.312(e) (1). A provider and health plan would need to address the terms of the health plan's data access and limits thereof and agreement with the health plan. The transmission of information electronically would need to meet 45 CFR Part 162 requirements for transmitting electronic referral information (162.1301) and other standards as required, including the minimum necessary standard. An additional variable to consider in the payment scenario is workers' compensation, where the parties have rights of appeal on treatment issues from a Managed Care Organization (MCO) to the Bureau of Workers' Compensation and to the Industrial Commission [See OAC 4123-6-16; ORC 4123.511]. Limiting access to records the MCO reviewed in making its initial determination may pose due process problems, since Ohio WC is a governmental function. In addition the VWG and LWG identified the following observations relevant to scenario 5. Authorization is required under HIPAA for psychotherapy notes 45 CFR 514(d)(2). Ohio law prohibits disclosure of HIV status without authorization (ORC 3701.243). State workers' compensation statute governs disclosure for WC benefits 45CFR 512(l); O.A.C §4123-6-20(D).

2.3 RHIOs (Scenario 6)

2.3.1 Stakeholders: Regional Health Information Organizations, RHIOs, physicians, consumers and other health care providers

2.3.2 Domains: The primary domain for this scenario is Information Use and Disclosure policies. *Role Based Access,* defining who has access to information at a specific level is the principle business practice. The disease management issue described in this scenario, while not specifically stated as such, could have research ramifications and falls into the same area as the *Research Request* business practice identified in Scenario 7. The monitoring of each provider in the

manner of treatment is a quality review practice that is typically done by health care payers not RHIOs. This scenario does not specifically state the data is required for research purposes. If the use is for research purposes, the RHIO board would provide a mechanism for review of all report requests and would follow IRB protocols with respect to aggregate data and reports.

2.3.3 Critical Observations: A RHIO is a neutral trusted third party intended to facilitate effective health information exchange to improve the quality of patient care by providing comprehensive information at the point of care. Each RHIO board will have to establish business rules about the types of data usage that will be permitted. It is interesting to note that two of the Ohio RHIOs (Dayton and Athens) are administratively housed in Schools of Medicine with already established business rules, IRBs, and other institutional supports. Some RHIOs provide reports back to user organizations to facilitate and encourage self-monitoring. However information, like that described in the ranking of providers, would likely jeopardize the neutrality of the RHIO. Existing Ohio RHIOs use aggregated information in community health planning; for example responding to the needs of the uninsured and underinsured, health risk factors, etc. In this scenario, the fulfillment of the first item is, "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." There is no reason to maintain patient identifiable data to assess the management of diabetic patients as a class. In current practice, Ohio RHIOs would only use aggregate or de-identified information to evaluate treatment or outcomes. Trends are analyzed for public health and other planning purposes. Recognizing that disease management is a complex process that includes the patient, environment, health care providers and health educators, the only effective response must focus on all of those systems, not target only one. The second item in the scenario description, "…the RHIO also intends to monitor participating providers to rank them for the provision of preventive services to their diabetic patients," is unlikely to occur in existing RHIOs given the need for neutrality and interest in promoting broad participation. The only way this might work would be to provide information confidentially to practices and providers. This would provide a self-evaluation process with data for each practice benchmarked against a set of community level data. The underlying difficulty with this scenario is that it assumes that health information exchange will be limited to existing paradigms, ones that look at diseases, transactions and "bits" of health information. This bifurcated view of health and health care does not support the new paradigm of patient centric health care. A holistic view of patients in the practice of medicine is necessary to integrate health knowledge management into the practice of medicine.

Because the RHIO is not a covered entity or an organized health care arrangement, patient authorization meeting HIPAA requirements would be required for a participant organization disclosure to the RHIO unless the information is used and disclosed pursuant to a HIPAA compliant business associate agreement. If no BA agreement is in place, patient authorization to use and disclose would be a significant barrier 45 CFR 164.502(e), 45 CFR 164.508.

2.4. Research (Scenario 7)

2.4.1 Stakeholders: The primary stakeholders include: Hospitals, Clinicians, Consumers, Laboratories, Government Payers and Research Sponsors, Private Payers, and Other Corporate Research Sponsors.

2.4.2 Domains: The primary domain identified for this scenario is Information Use and Disclosure Policy. There are two principle business practices to consider. The *Research Request* business practice asserts that all research projects fall under the auspices of the Institution Review Board (IRB). *Deviation of Intent* addresses the practices followed should variations arise to the original intent of the research project. Should the need for variations arise, the practice requires re-submittal to the IRB for additional approval. The Common Rule, 45 CFR 46.103(b) requires that an IRB review and approve research involving the use of human subjects or individually identifiable health information. In addition to the Privacy Rule's individual authorization requirement, the Common Rule requires that a signed consent be obtained from potential research subjects, which explains the potential benefits and risks associated with their participation in the study.

2.4.3 Critical Observations: The Health Insurance Portability and Accountability Act (HIPAA) Standards for the Privacy of Individually Identifiable Health Information (the Privacy Rule) require that a prospective research subject execute a written authorization to allow an investigator to use a subject's individually identifiable health information for research purposes, including incorporating the information into an electronic database for the study. In the case of minors, a parent or legal guardian must complete the HIPAA authorization on the child's behalf. The authorization must describe, with specificity, what the health information will be used for, who will have access to the information (including, for example, the principal, the co-investigator, the institutional review board (IRB) reviewing the research, the sponsor, and federal oversight agencies such as the Food and Drug Administration), how long the information will be used, and that the subject's health information will be placed in a database for the project.

The HIPAA Privacy Rule requires that an authorization describe to subjects who will have access to their individual health information used in the study, as well as how long the information will be kept or used. Similarly, the Common Rule requires the IRB to approve the study methodology, including how the database will be accessed, used and secured. Both the Privacy and Common Rules, however, provide mechanisms that allow the use of study data by researchers not included in the original IRB-approved protocol and disclosed to subjects in the HIPAA authorization. Specifically, both the Privacy Rule and guidance from the federal Office of Human Research Protections allow the research data to be de-identified and provided to the postdoctoral fellow for use in a white paper not related to the original research. In order to provide individually identifiable health information to the fellow, however, the principal investigator must obtain re-consent and authorization from the subjects for use not included in the original protocol and authorization. The Rules also provide a mechanism for the investigator and fellow to formally request a waiver of individual authorization and informed consent from the IRB - if specific criteria including the Rules are met. The federal Food and Drug Administration (FDA) Policy for the Protection of

Human Subjects, however, does not generally allow waivers of informed consent. As a result, the white paper could not be used to support a new drug application submitted to the FDA.

If an investigator wants to extend the length of the study to collect and track personal health information beyond the time frame specified in the consent and authorization and approved by the IRB, the Privacy Rule and the Common Rules requires that subjects consent to the proposed additional use. As noted previously, both the Privacy Rule and Common Rule, however, allow the principal investigator to request a waiver of individual authorization and consent from subjects if the specific criteria in the Common Rule are met. Such criteria include the practicability of obtaining re-consent as well as the nature and risks and benefits associated with the proposed additional use. In this scenario, however, a waiver is unavailable, since the research involves the study of a new ADD/ADHD drug, which is regulated by the FDA. As a result, the principal and/or co-investigator will likely need to again obtain consent from the subjects and their parents or guardians in order to collect individual health information for an additional six- month period. 45 CFR 46.101, 21, CFR 50.20, 21, CFR 50.23, 45 CFR 164.512, and Department of Health and Human Services Office for Human Research Protections August 10, 2004 Guidance on Research Involving Coded Private Information or Biological Specimens

2.5 Law Enforcement (Scenario 8)

2.5.1 Stakeholders: The primary stakeholders include: Hospitals, Clinicians, Consumers, Laboratories, Payers and Government

2.5.2 Domains: There are two primary domains, Information Use and Disclosure and State Law that are applicable to this scenario. Three business practices have been identified for this scenario. The first, *Request by Law Enforcement* addresses the need to validate a request from law enforcement to release patient information without a client authorization. To release the patient's blood alcohol test results to the police officer pursuant to HIPAA 45 CFR 164.512(f)(1), the disclosure would have to be required by state law, or pursuant to: a court order or subpoena or summons issued by a judicial officer, grand jury request, or an administrative request (administrative subpoena, summons, authorized investigative demand) that is relevant and material to a legitimate law enforcement inquiry, specific and limited in scope and not able to be provided in a de-identified format. To be a required disclosure under state law (ORC 2317.022), the officer would have to submit a "written statement requesting the release of records" indicating that an official criminal investigation has begun regarding a person, pursuant to Ohio law. The second business practice, *Request from Law Enforcement,* pertains to law enforcement access being limited to specific electronic records that are the subject of the request because it is not authorized to view entire medical record. The third business practice identified by the work groups is *Authorization Review.* Pursuant to HIPAA, the parents of an adult child are not permitted to review the Emergency Room record and laboratory results unless the patient signs an authorization allowing for the disclosure OR the parents have been designated by the son as his "attorney in fact" in a durable power of attorney for health care and he was not competent to make his own health care decisions per 45 CFR 164.502(g)(2).

2.5.3 Critical Observations: Parents of an adult child are not permitted to review the Emergency Room record and laboratory results of that child unless the patient signs an authorization allowing for the disclosure 164.508(a) OR the parents have been designated by the child as an "attorney in fact" in a durable power of attorney for health care and the child was not competent to make his own health care decisions per 45 CFR 164.502(g)(2). In addition, the parent's receipt of Explanation of Benefits from their insurance company often contains enough descriptive information about billing for the health care service to enable parents to learn medical information to which they would not otherwise be entitled. This situation can be a barrier to care if a person decides to forego care because a related or unrelated third party is responsible for payment. One final note, the Federal Drug and Alcohol Confidentiality Act does not apply to most general emergency room visits 42 CFR 2.12(e)(1).

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

2.6.1 Stakeholders: The primary stakeholders for scenarios 9 and 10 include: Clinicians, Payers, Clinics, Consumer, Pharmacy, and Behavioral Health organizations

2.6.2 Domains: The domains identified for these scenarios are Information Use and Disclosure and User and Entity Authentication. There are several business practices that were identified as applicable to both scenarios. The first business practice *Patient Authorization and Verification of Access* addresses the requirement to obtain permission from the patient to share information with an appropriate business entity. There must be a process to validate appropriate use by an entity prior to accessing a specific class of patient data. The patient authorization to release information must be specific and based on needs of the sharing entities. The second business practice is a repeat of the need to create an appropriate *Business Associate Agreement.* The agreement is required to permit sharing of information between the hospital/provider entity and the Pharmacy Benefits Manager (PBM). Consistent with the BAA is the business practice to provide *Minimum Necessary Release of Information that* is a HIPAA requirement under 45 CFR 164.502.

2.6.3 Critical Observations: In reviewing theses scenarios the work groups expressed several concerns. First, they expressed concern over the method for exchanging and receiving the request for information. Members of our stakeholder community suggested a telephone call with call back procedure was sufficient to satisfy user authentication. Others suggested the request should be made by fax. To that end, ORC 4729.37 and OAC 4729-5 contemplate phone and fax contacts and set forth the procedure and record keeping requirements. 45 CFR 164.312 requires reasonable measures to safeguard electronic transmission of PHI. Secondly, they noted that the procedures may result in a delay to treat the patient. In addressing this concern, 42 CFR 423.566, .568, .570 and .578 requires timely benefit determinations, expedited coverage decisions and exceptions. Thirdly, they noted concern regarding the potential for the PBM to be outside the patient area of residence. In such a case, if the PBM has entered into a contract with an Ohio employer to provide services to Ohio residents, to the extent applicable, the PBM would be subject to Ohio law. The hospital as a self-insured employer is subject to ERISA requirements concerning

the proper administration of its health plan. The PBM as a subcontractor of hospital should be required to follow the same ERISA rules.

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

2.7.1 Stakeholders: The primary stakeholders in scenarios 11 and 12 are consumers, hospitals, and clinicians.

2.7.2 Domains: The principle domain is Information Use and Disclosure and there are two principle business practices of note. *Request for Review* provides the Privacy officer will review all requests for information from the Marketing Department. The concern is for the level of consent required to satisfy the request. This depends on the nature of the integrated health delivery system. If ABC Health Care itself is a HIPAA "covered entity" (as opposed to holding company or corporate entity that does not provide covered services), it (along with its affiliated hospitals) could be part of an organized health care arrangement (OHCA) or an affiliated covered entity (ACE) under HIPAA. In such case, the use and disclosure of PHI by ABC (as part of the OHCA or ACE) would be the same as use and disclosure of the affiliated hospitals. If ABC Health Care is not a covered entity, the communication activities must emanate from the hospital (i.e., covered entity) level. The first consideration is whether the critical access hospital can disclose PHI to DEF Medical Center for DEF's "health care operations" under 45 CFR 164.506(c)(4). If the covered entities cannot share/disclose PHI, each of the hospitals must make the communications with its own patients.

The definition of "marketing" under HIPAA is the key to the analysis of whether these communications are permissible under HIPAA. Under 45 CFR 164.501, "Marketing" does not include communications "(i) to describe a health-related product or service ...that is provided by...the covered entity making the communication,...or (iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual." Thus, it would appear that DEF could make the communication with all patients (assuming it properly received the PHI as part of an OHCA, ACE or for health care operations) under clause (i) above -- or each of the affiliated critical access hospitals could make the communication as a recommendation of "alternative health care providers or settings of care" under clause (iii) above. The second, and perhaps more significant business practice, involves securing the *Patient Authorization.* Our stakeholders suggest it is the Marketing Department that has primary responsibility for securing the patients' release to use their information pursuant to CFR 45 164.508.

2.7.3 Critical Observations: Patient authorization is not needed for the hospital to send information to its patients concerning the services available at the hospital. See 45 CFR 164.501 (definition of "marketing"). Providing patients with information on the hospital's new pediatric wing/services is a permissible purpose and is not considered "marketing" for HIPAA purposes. Under 164.501, "Marketing" does not include communications "(i) to describe a health-related product or service ...that is provided by...the covered entity making the communication." Based on OCR guidance, it appears that these

communications can be targeted to patients of the hospital who recently gave birth. The Privacy Office and Marketing Departments must determine what mode of transferring information will be used and the type of information, i.e., identifiable or de-identified information will be provided to the marketing department. Resolution of this issue will depend on the facts, which should be analyzed on a case-by-case basis, but the activities described can be undertaken without de-identifying the PHI if all applicable HIPAA requirements are met (e.g., the minimum necessary standard). Thus, a minimal barrier may exist, but this barrier already exists (regardless of EHR implementation).

Additional concerns were raised regarding the disclosure of health information of Medicaid recipients. Even in that regard there was not unanimous consensus on how the rules are applied. Proponents of the application of the rules in the scenario noted that essentially, the 42 CFR 431 Subpart F (Entitled Safeguarding Information on Applicants and Recipients) restricts disclosure of information to "purposes directly connected with the administration of the plan." Those are defined as establishing eligibility, determining the amount of assistance, providing services for the recipients (within the plan — which means the state plan, or the state's Medicaid program), and assisting or conducting investigations, prosecution of civil or criminal proceedings related to the administration of the program (42 CFR 431.302). The subpart requires that the Ohio Department of Jobs and Family Services (ODJFS) have restrictions in place and that the restrictions apply to those to whom the information is released that require them to be under the same standards of confidentiality as the agency itself. Thus, the hospital is under the same standards of release of the information as ODJFS (42 CFR 431.306). The types of information subject to the safeguards includes names and addresses, medical services, social and economic conditions, evaluations of personal information, medical data (including diagnosis and past medical history), information received for verifying income eligibility, and any information regarding identity of third party resources (42 CFR 431.305). There is also a requirement similar to the HIPAA requirement that only the minimum necessary information be released if the conditions are met for such release. Ohio Revised Code Section 5101.27 covers not only Medicaid but all public assistance programs and restricts the release of information to the recipient, an authorized representative, legal guardian, or the attorney of the recipient (but only if there is written authorization that complies with ORC 5101.271). ORC 5101.27(D) permits the release of information if the recipient provides voluntary, written authorization and the release is permitted by federal law. ORC 5101.27(F) permits the release by the agency (and by extension, and through the provision in the provider agreement that subjects a provider, including a hospital, to the same confidentiality restrictions of the agency) if the release is for purposes "directly connected to the administration of or provision of medical assistance provided under a public assistance program" and the information is released to an entity subject to the standards of confidentiality comparable to those of the agency.

An alternative viewpoint on the 42 CFR 431 Subpart F issue is that it does not specifically apply to health care providers. Rather, it is federal law imposing requirements on state Medicaid agencies. It requires a state Medicaid agency to adopt rules to govern its own practices to ensure that

it safeguards the information of its applicants/recipients. The law cited as authority for binding providers to the state Medicaid agency standards (42 CFR 431.306) provides in the pertinent subsection (b): “Access to information concerning applicants or recipients must be restricted to persons or agency representatives who are subject to standards of confidentiality that are comparable to those of the agency.” In the absence of specific law governing health care providers, this provision does not appear to provide definitive authority for the proposition that all health care providers must adopt separate policies for the use and disclosure of the protected health information of Medicaid applicants and recipients.

2.8. Public Health/Bioterrorism (Scenario 13)

2.8.1 Stakeholders: The primary stakeholders are clinicians, Physician Groups, Federal Health Facilities, Hospitals, Payers, Public Health, Community Clinics, Lab, Pharmacies, LTC, Hospice, Correctional Facilities, State Government, Trauma Centers, and Poison Control Centers.

2.8.2 Domains: The primary domain for this scenario is State Law Restrictions. The business practice identified is *Reporting a Bioterrorism Event.* This practice involves an entity making a telephone call notification of a possible event followed by fax verification to state authorities. Boards of health, health authorities or officials, health care providers in localities in which there are no health authorities or officials, and coroners or medical examiners shall report promptly to the department of health the existence of any of the diseases or illnesses listed in Ohio Administrative Code 3701-3-02. The individually identifiable health information reported to public health agencies is protected (confidential and not subject to disclosure) pursuant to R.C. 3701.17. Additionally, pharmacies, poison control centers, and other health-related entities are required to inform public health agencies of unusual events per R.C. 3701.232 and 3701.201. However, during an actual terrorism event, the Federal Bureau of Investigations will be the lead agency, under Presidential Decision Directives 39 (1995) and 62 (1998); see, 10 USC 382, 18 USC 175-178, 18 USC 2331-2339B. Communication and the transfer of data outside public health or hospitals will occur on an "as needed" basis and will be conducted primarily via telephone and secure facsimile transmissions. In that regard, timing of required communications are governed by Ohio Administrative Code 3701-3-05 and 3701-3-06. Additionally, HIPAA requires an accounting of the disclosures and procedures. See 45 CFR 164.528.

2.8.3 Critical Observations: The means and timing of communicating information on reportable disease cases is set forth in Ohio Administrative Code 3701-3-05 and 3701-3-08. In Ohio it is generally believed that all entities are aware of the State reporting procedures and can find additional information at"

"Know your ABCs" – **http://www.odh.ohio.gov/pdf/idcm/intro9.pdf** ;

"Infectious Disease Control Manual" - **http://www.odh.ohio.gov/healthresources/infectiousdiseasemanual.aspx.**

There are no legal barriers preventing the exchange of information in this scenario, however, an attitudinal barrier exits. Some providers refuse to comply with state reporting requirements.

2.9. Employee Health (Scenario 14)

2.9.1 Stakeholders: Hospital, Payer, Consumer, Payer and Clinician

2.9.2 Domains: There is one domain associated with this scenario, Information Authorization and Access Control and two primary business practices. The first practice is *Authorization to Release Information* and involves obtaining patient authorization to release information for purposes other than treatment, payment or health care operations (TPO). HIPAA-compliant patient authorization is required for this non-TPO purpose, which should be easily obtained because the disclosure is for the patient's benefit **(**See 45 CFR 164.508). If a hospital has patient authorization there is no barrier to electronically generating a return to work document to be given to a patient or to an employer or other party per the patient's authorization.

The second business practice is the *Data Transmission Protocol* and involves physician verification that the patient can return to work. The stakeholders in the work groups suggested this is currently accomplished through both voice and fax communications. The preference is to transmit over secure e-mail to a secure fax receiver. With respect to restrictions related to minimum necessary the terms of the authorization establish the limits of the PHI that can be disclosed. The minimum necessary standard does not apply to disclosures made pursuant to an authorization (See 45 CFR 164.502(b)(2)(iii).

2.9.3 Critical Observations: A cut and paste approach referenced in the scenarios does not pose legal problems, provided that the PHI that is cut and pasted meets the requirements of the authorization. A possible exception to this is that the covered entity must ensure that metadata or hidden text is not transferred during the cut and paste process. A practical problem may exist because it would seem more likely that PHI beyond the scope of the authorization could be inadvertently included in the disclosure if a cut and paste process is used. Members of our work group noted that problems that arise in this area are often due to follow-up calls from employers that seek additional information regarding the employee/patient. Providers (and their staff) need to ensure that all PHI disclosed during follow-up conversations/disclosures is within the scope of the authorization allowing the initial release of the PHI.

2.10. State Government Oversight (Scenarios 15–18)

2.10.1 Stakeholders: Public Health, State Government, Consumer, Law Enforcement, Clinicians, Hospital, Laboratory, Behavior Health, Community Clinics and Health Centers, Medical and Public Health Schools and Public Health Agencies

2.10.2 Domains: The primary domains for scenarios 15-18 include: State Law Restrictions, Information Authorization and Access Controls, and Information Transmission Security or Exchange Protocols. There are a number of business practices including *Exchange of Health Information* which identifies the processes for exchanging information among multiple entities within the State; *Mandatory State Requirements* that defines State requirements for reporting mandated screening tests for infectious disease; *Minimum Necessary Guidelines* as discussed previously in this report; *Authorization to Treat* and the requirement to obtain authorization from a patient prior to treatment protocol; *Alternate Authorization* that addresses the requirement for a BAA in the absence of patient authorization; and *State Reporting* outlines the protocols for mandatory reporting.

Under Ohio statutes and regulations, medical providers and laboratories are required to report diagnoses or laboratory results that identify a communicable disease listed in state regulations to local and state health officials. These diseases are considered by public health officials to represent a danger to public health. RC 3701.23 and OAC 3701-3-01 et seq.; see R.C. 339.78. The director of the Ohio Department of Health (ODH) has statutory discretion to share information necessary to "control, prevent or mitigate disease." RC 3701.14(J); see RC 3701.17 and 339.81. ODH works with other state health departments and the Centers for Disease Control and Prevention, with the latter's authority at 42 USC 264 et seq. and 42 CFR Parts 70 and 71. Federal and state statutes and regulations enable governmental response to communicable, infectious diseases to be appropriate to the size of the risk. There are no obstacles other than risk for inappropriate response by public or private parties. Substantial state and federal legal authority exists that enable state and local health departments to screen for communicable disease, mandate treatment, provide for isolation or quarantine, share PHI with persons or entities necessary to control, prevent or mitigate disease, and utilize law enforcement to enforce. Such authority enables government to screen and manage such situations irrespective of a patient's mental health.

Regarding scenario 16, Ohio does not use an Interactive Voice Response System for newborn screening because it cannot verify the caller (the person or entity). As the official testing laboratory for Ohio, ODH receives actual blood spots from providers and then faxes results of screenings to the submitting providers. To ensure accurate communication and given the insecurity of email, ODH maintains a self-identified facsimile number for every provider. ODH puts responsibility for security of faxed information on the provider receiving the fax. The only alternative would be for each provider to own a mass spectrometer (the device needed for the testing) and ODH would only function as a results repository – could only have a completely electronic exchange of samples and results if every provider had the machine - defeats purpose of state lab doing the testing. Also, Ohio only performs limited tracking subsequent to newborn

screening. Confidential newborn screening results are sent to the birth hospital and to the physician of record.

With respect to Scenario 17, the shelter is not a covered entity under HIPAA and could therefore share information with the relative. The drug program could not share any information with the relative without an authorization pursuant to the Federal Drug and Alcohol Confidentiality Law (42 CFR § 2.33) and OAC 3793:2-1-06(H). The primary care physician could share information with the relative if the patient signs an authorization allowing for the disclosure OR the relative has been designated by the patient as his "attorney in fact" in a durable power of attorney for health care and he was not competent to make his own health care decisions. The drug clinic would need a client authorization or a Business Associate Agreement/Qualified Services Organization agreement with the county to share information with the county for the purposes of program reimbursement pursuant to the Federal Drug and Alcohol Confidentiality Law and Ohio law.

2.10.3 Critical Observations: Several issues arise from this collection of scenarios that the VWG and LWG chose to address. With respect to scenario B and newborn screening and whether or not newborn screening data can be transmitted electronically the groups found the newborn screening statute renders the information confidential. Results are sent to the birth hospital and to the physician of record (POR). The Ohio Department of Health security policies and procedures are stricter than the HIPAA security rule standards because of terrorism issues. No state law mandates a tracking disclosure of PHI or authorizes a public health authority (Ohio Department of Health) to track the child over time. This is a potential privacy concern barrier because no law governs should the state wish to conduct tracking over time. ODH does some follow-up to make sure the child is referred to a care provider but management of care is left to care providers. See ORC 3701.501 et al., OAC chapters 3701-55 and 3701-36, and 45 CFR 164.512 (a) and (b).

With respect to Public Health Scenario C the VWG and LWG identified that the shelter is not a covered entity and could share its information with the relative. The drug program could not share any info without an authorization 42 CFR § 2.33, OAC 3793:2-1-06(H). The primary care physician (PCP) could share information with the relative if the patient signs an authorization allowing for the disclosure 164.508(a) OR the relative has been designated by the patient as his "attorney in fact" in a durable power of attorney for health care and he was not competent to make his own health care decisions. Also based upon the facts presented, there may be an additional potential legal obstacle in scenario 17. The facts presented do not indicate whether the homeless man receives public assistance. The fact that the man has a primary provider and the statement that the man is to be sent to a hospital-affiliated drug treatment facility "for his addiction under a county program" lends credence that the homeless man may be receiving public assistance, which may include a public medical assistance program or Medicaid coverage for medical assistance. If the homeless man does receive a medical benefit through a public medical assistance program the confidentiality statutes may restrict the release of information. ORC 5101.27 addresses all public assistance, including Medicaid. If the homeless man receives, or is eligible for, Medicaid, confidentiality of information is also subject to 42 CFR 431 Subpart F and OAC 5101:1-37-01.1.

Regarding Scenario 18, Health Oversight, the VWG and LWG noted significant barriers with respect to most aspects of the contemplated information exchange: 1) there are few, if any, common formats and identifiers in order to allow for meaningful exchange of information among agencies and between several states which affects tracking processes; 2) there are barriers imposed by requirements for business associate agreements, data use agreements or governmental memoranda of understanding; 3) Medicaid regulations may preclude the disclosure of some of the information; 4) the Family Educational Rights and Privacy Act (FERPA); 34 CFR Part 99, applies to educational records and may be implicated by this scenario – FERPA's privacy protections are not entirely consistent with HIPAA, authorization/consent will likely be required by parents for the release of the educational record, though there is an exception that may or may not apply to this scenario (34 CFR 99.31 permitted disclosures in cases of health and safety emergency). Additional regulations that may apply include: 42 CFR Part 431 Subpart F Safeguarding Information on Medicaid Applicants; state laws and regulations restricting the release of information regarding recipients of public assistance programs including Medicaid; ORC Section 5101.27 and OAC Section 5101:1-37-01.1; and HIPAA restrictions and requirements for uses and disclosures of protected health information at 45 CFR 164.502, 164.504, 164.508, 164.512, and 164.528.

3. Summary of Critical Observations and Key Issues

Over the course of this project the Variations Working Group and Legal Working Group were able to identify a number of key issues that impact the HISPC efforts. They include the following:

- The single largest obstacle to open information exchange and interoperability is a lack of credible data standards shared by all stakeholder entities. Numerous efforts have been made including the HL7 initiative; however, resistance from the software development industry has kept this issue unresolved. Until standards for data exchange, including consistent data formatting and exchange protocols are adopted, this issue will remain unresolved, and the opportunity to enact true systems integration will remain unfulfilled.

- There are relatively few legal obstacles preventing the exchange of electronic health information. Adoption of the HIPAA guidelines has provided the individual states an opportunity to develop internal standards for patient privacy and security. In many cases the state standard exceeds that mandated at the federal level providing a higher expectation for securing the health record. This does create some differing standards, however, that must be reconciled in practice.

- There is widespread consensus that the patient electronic health record can contribute to improved management of ones individual health. The challenge is to develop systems that are affordable to all levels of the health care delivery system. Adoption of this tool is occurring in the larger delivery systems supporting an urban community. However, adoption in the rural areas has lagged behind the urban communities principally as a result of limited funding.

- Lack of a standardized patient identifier is inhibiting electronic exchange of information. Disparate systems with identifiers unique to the individual systems have limited interoperability, creating inefficient interfaces, and jeopardizing the integrity of the data exchange.

- Universally, the physician members of the work groups suggested that treatment of the patient is the first priority in an emergency and obtaining consent or other administrative task is not a primary consideration.

- As a general rule the groups agreed there is a need for a consistent method to authenticate a user request. This can be easily accomplished through the use of fax technology or through more sophisticated use of network devices using standardized login protocols.

- Use of the HPIO wiki site proved to be a valuable tool for the dissemination and collection of data and for providing information to the general community at-large.

- Ohio law requirements that are applicable to mental health records and stricter than HIPAA, and the very restrictive requirements of the Federal Drug and Alcohol Confidentiality law that are applicable to alcohol and drug abuse patient records, pose an additional challenge to the exchange of health information.

- Effective, statewide and national health information exchange will only be successful when there is a major commitment from the state and federal government to find mechanisms for funding the necessary initiatives that will enable exchange. In Ohio we observe that no single health care sector is positioned or able to provide the necessary funding to jump start health IT or exchange of information. There does not appear to be sufficient collective will in the private sector to fund health information exchange outside of localized efforts where return on investment can be quantified. Even then, some sectors cannot afford the investment that is necessary. The private sector is not likely to step up to the plate unless there is significant public sector financial support to fund well articulated policy objectives.

4. Appendices