Draft # 3 Interim Solutions Report:

Section 1 - Background

1. Description of the purpose and scope of this report:

The purpose of this report is to document privacy and security solutions identified by Ohio aimed at addressing barriers to health information exchange (HIE) that result from organization-level business practice, policies and laws and regulations that underlie them, and that were identified and documented by the Ohio Variations Workgroup (VWG). These solutions seek to preserve essential privacy and security protections, and are conceived to facilitate implementation of the National Health Information Network.

The Ohio Interim Solutions Report will document the process used to develop solutions, including the organization of the Ohio Solutions Workgroup (SWG), its charge, membership and stakeholder representation, the process for identifying and proposing potential solutions, the way the state will vet, evaluate and prioritize proposed solutions, and their feasibility for implementation.

The Ohio Interim Solutions Report will also document each of the identified potential solutions in the context of HIE, the privacy and security domains affected, stakeholders involved, HIE barriers being addressed, stage of development and use of solution, and possible barriers to adoption.

2. Description of level of HIT development in Ohio:

In the State of Ohio the level of adoption of HIT is on an upward trend. Large hospital systems are purchasing enterprise solutions for HIT, and most are in the process of implementing those systems; none are fully implemented. All of these organizations have the expectation that their vendor will provide an interoperable solution. While large physician practices have in some cases adopted EHRs and some small physician practices have EHRs, other physician practices may have practice management systems, but lack EHRs. Ohio's physicians see the benefit to EHRs, but generally perceive the cost of such systems as prohibitive. Many physicians who are hospital affiliated expect their hospital to provide them with an EHR or help subsidize implementation of EHRs in their offices to integrate into (Regional Health Information Organization) RHIO systems being implemented across the state.

In the broader arena of health information exchange, the State of Ohio has the Third Frontier initiative, a publicly funded effort to promote development and dissemination of cutting edge information technology across the state. Since 2002, Ohio's Third Frontier Project has invested more than $207 million in 15 biomedical public-private commercialization partnerships, ranging from cardiovascular, cancer, and neuromodulation, to imaging, stem cells and bioinformatics. Home to the NCR Corporation, with its Teradata products that provide advanced data mining and eliminate concerns about scalability in systems, Ohio is positioned to model solutions for many industries, most particularly health information technology. The State of Ohio has committed $1.6 billion over the next seven years in support of technology-based economic development.

Ohio is working toward statewide coordination of HIE through public forums hosted by the Health Policy Institute of Ohio, and through developing Regional Health Information Organizations across the state, two of which are currently actively engaged in health information exchange. In October 2005, the Health Policy Institute of Ohio (HPIO) published "Assessing Health Information Technology in Ohio: Briefing Paper for the 2005 Health Information Symposium." This monograph documented specific HIT and HIE projects across the state including electronic records systems at multiple levels of development in 13 hospitals and several hospital systems, as well as four large physician groups. Also documented were three research projects in HIT two of which were funded by Agency for Healthcare Research and Quality (AHRQ) and one through an Ohio philanthropic organization involving pilot projects in e-prescribing and disease management programs. HPIO has also coordinated the creation of an HIT/HIE Roadmap for Ohio with input from a broad stakeholder base, and is providing state legislators and the new governor's office with recommendations for moving forward with statewide coordination and monitoring of HIE efforts. Interest in Regional Health Information Organizations (RHIOs) has grown across the state and current efforts are summarized below.

In Dayton, the Center for Healthy Communities (CHC), a division of Wright State University Boonshoft School of Medicine, has implemented an electronic shared, community-wide health record based on the Continuity of Care Record standard. This central data repository, called HIEx™, now houses patient and household-centric demographic and health data on 26,000 individuals. CHC is also the lead organization in the HealthLink RHIO, which involves some thirty organizations providing data on paper and referrals to Community Health Workers, and five organizations routinely exchanging health information and clinical data.

Cincinnati is home to HealthBridge. HealthBridge is an internet portal through which more than 100 entities supply, and thousands of users retrieve, laboratory reports in a standardized format, developed through the collaboration of the members. The HIE has several critical components, including secure connections between physician organizations and hospitals, access to existing hospital information and a community-wide clinical messaging system. Data from multiple sources are standardized across the community and delivered electronically to physicians. Information is currently physician-centric and remains in the central database.

The Community Health Alliance of Northwest Ohio (Toledo) is clinically focused and patient focused. The infrastructure includes a neutral community-centric data processing center, and a highly leveraged service center. Key components of the system are the consistent identification of each patient across institutional boundaries, and the automatic distribution of information between care sites according to privacy-protected routing rules.

Many groups in the northeast area of Ohio (Cleveland, Akron, Canton, and Youngstown) are engaged in activities to promote the effective adoption of health information technology and health information exchange (HIE). This work includes individual projects aimed at promoting greater use among long term care facilities, among small physician practices, and between federally qualified health centers and the region's major hospitals. In addition, several Cleveland hospitals compose the third community of the Northrup Grumman AHRQ award to develop HIE architecture (the University Hospital, Cleveland Clinic, and MetroHealth hospital systems). In 2006 the Cleveland Akron area created NEORHIO.

In central Ohio, three major health systems, The Ohio State University Medical Center, Ohio Health and Mt. Carmel Health System along with Select Specialty Hospitals have a Clinical Working Group that is in the process of developing a clinical transaction based on the Continuity of Care Record concept. The initial stages of the project will focus on the transfer of demographic and clinical data on patients being referred from one of health systems to a Select Specialty facility. The technology partner in this project is HTP, Inc. who will provide the transaction processing. The project is working to establish proof of concept and return on investment (ROI). Later phases will move towards more interoperability between these sites and other members and look at expanding the services to the members.

In the heavily rural southeastern part of the state, the Appalachian Regional Informatics Consortium (ARIC) has been funded by the National Library of Medicine; funding has supported planning activities for a nine-member coalition. The consortium's mission is to create a sustainable and replicable model for advanced integrated information management systems for rural health care in Appalachian Ohio. The model will establish a formal organizational structure and a comprehensive technical plan for a shared medical information system to benefit primary and behavioral health care providers, biomedical researchers and medical educators.

3. Description of report limitations :

The Solutions Working Group (SWG) has sought broad inclusive representation of all stakeholder groups and publishes all meeting minutes and materials on the pbwiki website http://hispc.pbwiki.com/ for the group. Meetings may be attended in person or via toll free teleconference. All working documents are e-mailed to all group members and all are encouraged to share materials with other interested parties. As a consequence the outreach process has been very effective; the resultant feedback has been from stakeholders with strong interest in these items. With the numerous and varied methods used to collect input, we can only assume that silence asserts agreement. With almost 50 members on this group from all stakeholder groups, we assess that we have achieved broad stakeholder input and review. (Member list attached as Appendix A)

Section 2 - Summary of Interim Assessment of Variations Report

1. Brief description of the main findings from the interim assessment of variations report, including the top 5 to 10 identified barriers

Several significant findings were identified by VWG 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.

2. Description of 'effective' practices identified by the state, including overall practices that ensure improved electronic health information exchange (and that cut across multiple domains specified in the contract) as well as practices identified within each of the nine domains (a brief description of the definition of 'effective' practice should be provided)

Establishing RHIOs around the State's major population centers administered by neutral and trusted third parties is pivotal to secure exchange of information. The two RHIOs currently exchanging data use standard HIPAA procedures (Business Associate Agreements and Data sharing agreements) to establish privacy and security parameters and responsibility. The two RHIOs that exchange electronic information are Healthbridge in Cincinnati (the result of a successful CHIN effort) and HealthLink RHIO in Dayton, (the result of a HRSA HCAP grant).

HealthLink RHIO and ARIC in southeastern Ohio are both housed in schools of medicine that have been well established as conveners of successful collaborative efforts. Ohio's schools and colleges of medicine have provided a validated and trusted third party with no ostensible institutional gain beyond further research into the practice and science of medicine. The knowledge resources of these institutions have been used to successfully accelerate the process of establishing and focusing local RHIO efforts.

The ongoing dialogue about health information technology and exchange that HPIO has supported now for the past three years has focused the attention of governmental, private and public hospitals, professional organizations and consumers on these topics.

Absent consistent standards for electronic reporting of quality measures from hospitals, the Ohio Hospital Association has established a process of collecting data from most hospitals around the state, centralizing and providing a kind of standardization of data reporting for the purpose of performance and quality review. The data arrives in non-standard form, is standardized, deidentified and shared with hospitals for their own quality review processes. Several regional hospital based quality initiatives have effectively established regional inter-organizational reviews that have resulted in improved practices. This process sets an important precedent for HIE for the purposes of quality measures.

The Ohio Hospital Association in conjunction with HPIO and HTP Inc. have provided education on health information exchange. At its annual meeting last year OHA hosted representatives from the Utah Health Information Network who provided a presentation on their project with the hope that Ohio could organize a network as a starting point for health information exchange using the technology tools and lessons learned from Utah.

The Ohio State Medical Association, the Ohio Association of Family Practice Physicians and the Ohio Osteoathic Association have provided a strong physician voice in all of the statewide discussion of HIT and HIE.

The State Office of Information Technology has organized a Sensitive Data Protection Working Group with representatives from twenty-eight state agencies. Through an administrative rule promulgated under sections 1306 and 1347 of the Ohio Revised Code, the Office of Information Technology is discussing setting baseline security standards specific to sensitive data so that agencies and universities account for risks associated with the sensitive data they hold and establish certain protections, if they are not already in place. The Sensitive Data Protection Working Group will recommend protections for sensitive data held by the state and develop an understanding of what potential impact such protections may have. It is anticipated that the group will meet two to three times to develop and vet their recommendations for inclusion in the proposed Ohio administrative rule.

3. Lessons learned: brief description of business policies and practices that inhibit HIE because, for example, the policy or practice is too onerous

The three primary inhibitors of health information exchange are (1) the misinterpretation of HIPAA (2) the focus on health care payment transactions and (3) legacy data and systems requirements. HIPAA provides for release of information for treatment, payment or health care operations. However, the provisions of HIPAA are often misconstrued and variously interpreted. For example, existing industry practices have presumed ownership of health data by the institution or provider and not the patient, facilitating the rationale often put forward by hospitals of losing a “competitive edge” if HIE is routine practice. A second inhibitor is the reality that most current electronic health care data is transaction based, billing data, thus making payment and economics the drivers of health information exchange. This leads to the third inhibitor which is that providers have major investments of money and historical data related to payment transactions and claims. As they move forward with collecting and maintaining electronic clinical data, there is no precedent for HIE, and the required modifications in existing systems are expensive and time consuming, providing little incentive for changing existing practices in order to facilitate HIE. While it is clear that clinical data must be integrated with claims data, when technological platforms are based on messaging, the question of cost of integration must be balanced against net gained value. For example, most experts agree that claims data does not provide adequate information for clinical decisions, thus does not have informational (knowledge forming) value. Consequently in practice, electronic information silos are being established as a rapid pace, and electronic patient centric records that focus on clinical dimensions of care and are routinely exchanged across care settings to improve quality and reduce cost of care are in fact revolutionary.

4. Identification of variations identified by the state and NOT being addressed by the proposed solutions presented in this report

None

Section 3 - Review of State Solution Identification and Selection Process

1. Discussion of the overall process used by the State to develop solutions

The SWG met primarily during the month of November. They began by discussing the primary findings of the Interim Assessment of Variations Report (IAVR). Members were given the instruction that they were to review the IAVR and the pbwiki website in preparation for discussion of the six points (barriers) identified in the executive summary of the IAVR, and suggestions of solutions to respond to the barriers. Following each meeting, staff distributed minutes of these discussions and encouraged additional input between meetings. Staff then prepared an initial list of potential solutions generated during the meetings for review and comment. This initial list was also reviewed by the Steering Committee, who provided additional input. Following this, a draft of the Interim Solutions Report was circulated electronically to the SWG, followed by continued discussion both in meetings and electronically. The draft document was also posted on the pbwiki for broader review. All comments and additions were incorporated into the final draft for review by the SWG At the last meeting of the SWG, members of the Implementation Working Group were also present, and they will begin to identify ways to implement the various solutions proposed. Concurrently, the final draft of the Interim Solutions Report was reviewed by the Steering Committee for comment. Moving forward, this report will also be made available to stakeholders who attend the five regional meetings being held across Ohio during the month of December for further review and comment.

2. Description of the State Solutions Workgroup, its charge, membership and stakeholder representation

The State Solutions Working Group has been charged by the Steering Committee with identifying potential solutions to the barriers specified in the IAVR. The SWG has 46 members and has representation from all required stakeholder groups.

3. Description of the process used by the state to identify and propose solutions

The VWG report has set the universe of discussion for the barriers identified through that process. The SWG has reviewed those barriers and has suggested solutions that will be broadly reviewed by the LWG, VWG and stakeholders.

4. Description of the process to be used by the state to vet, evaluate and prioritize solutions

The Interim Solutions Report will be broadly distributed to solicit input from all interested parties and as the Implementation Planning Working Group continues its work, input will be sought to validate (vet) and to prioritize solutions.

5. Description of how solutions are organized and presented

Solutions are organized by barrier identified

6. Description on how state has determined the level of feasibility of identified solutions

The Implementation Planning Working Group will determine feasibility as they discuss implementation.

Section 4 - Analysis of State Proposed Solutions

Ohio Solutions to Assessment of Variations identified **barriers**:

Barrier: **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.**

Context: The barrier to insuring privacy and security of PHI through health information exchange identified here is lack of national standards. In fact, the national standards for privacy and security are outlined in HIPAA, however, the implementation of HIPAA varies extensively due to various interpretations, sometimes influenced by current practices, and enforcement of HIPAA compliance is understood to be a complicated process. In response, the Solutions Work Group proposes a number of solutions as follows:

Proposed solutions:

1 a. *National standards* not State standards are the solution.

1 b. The role of the State is to encourage consistent application of these national standards and encourage participation in the national standards setting bodies (i.e., ASTM, HL7, etc.) to assure broad representation and participation of all stakeholders on whom these standards and their application have impact. At the state level, *there should be a monitoring body that routinely reviews interpretation, compliance and practice related to the national standards*.

1 c. While HIPAA provides general national standards with regard to privacy and security, as *electronic messaging, elements of the clinical record, and transactions are increasingly electronic, national standards at this level should be adopted* to continue to support privacy and security protections, and to insure technical interoperability for ease of exchange across provider organizations.

1 d. As *national standards are implemented, they should be in compliance with the existing standards as defined by HIPAA.*

Domains:
3. Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises

4. Information transmission security or exchange protocols (encryption, etc.) for information that is being exchange over an electronic communications network
7. Administrative or physical security safeguards required to implement a comprehensive security platform for health IT
9. Information use and disclosure policies that arise as health care entities share clinical health information electronically

Types of HIE:
All data including clinical and billing data.

Stakeholders:
All:
Consumers
Government
Hospitals
Long Term Care
Medical Devices
Mental Health
Other Health Care Providers
Payers
Pharmacy
Physicians
Public Health

Stage of Solution:
Standards have been published for the Continuity of Care Record (CCR), HIPAA X12 transactions, NPI, and HL-7 messaging standards for version 2.x are in use.

Proposed solution in use by:
Standards setting bodies and the Office of the National Coordinator.

Appropriate for a wide range of stakeholders and HIEs:
Yes

Barriers to solution:
The standards setting process takes a great deal of time. The only comprehensive existing standard is the CCR and its adoption has not been encouraged or required.

<u>*Barrier:*</u> **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.**

<u>*Context:*</u> The barrier identified here has to do with the difficulty of accurately identifying and tracking every individual patient in a local, regional or national electronic health information network, and the potential for breeches in privacy or security if an individual's identity is compromised or inaccurate. Frequently, discussion in this area turns to the debate between a fully technical solution using a master patient index with a unique patient identifier, or the use of probabilistic matching using an algorithm of multiple bits of identifying information. The Solutions Work Group encourages a combination of the two as follows:

<u>*Proposed solutions:*</u>

2 a. Currently, there is a number that is unique and is applied to each birth certificate called a state file number. For every birth a unique number, which is comprised of a state code (2 digits), the year of birth (4 digits), and a unique number (6 digits) is created. It is a vital statistics sourced number currently used by the National Center of Health Statistics. The infrastructure to access information at the national level is being developed and managed primarily by NAPHSIS, the National Association for Public Health Statistics and Information Systems http://www.naphsis.org/index.asp Provisions for foreign born citizens of the US are also in place with this standard, however, there are not currently provisions for undocumented aliens and non-citizens in this country legally. The solution proposed is to *use the state file number as the primary patient identifier in the NHIN, with protocols developed for randomized probabilistic matching to routinely verify accuracy of this patient identifier.* Additionally, provisions will need to be made for people who access the health care system that are not currently captured by the state file number. A risk assessment of the use of any national unique identifier should be included.

2.b. Alternatively, and in the future, *accurate identification of patients should be through biometrics.*

<u>*Domains:*</u>
3. Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises

<u>*Types of HIE:*</u>
All

<u>*Stakeholders:*</u>
All:
Consumers
Government
Hospitals
Long Term Care

Medical Devices
Mental Health
Other Health Care Providers
Payers
Pharmacy
Physicians
Public Health

Stage of Solution:
The agreement to proceed with a unique identifier is still in question. Probabilistic models exist but must be adopted across platforms and systems.

Proposed solution in use by:
Vital statistics and public health

Appropriate for a wide range of stakeholders and HIEs:
Yes

Barriers to solution:
Agreement to use a unique identifier is absent. Probabilistic models must be standardized and adopted.

Barrier: **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.**

Context: The barrier identified here with regard to privacy and security of information through health information exchange is a variation on the lack of national standards barrier identified above, that there is not currently a national standard related to who has access to what information. While HIPAA outlines that information can be exchanged between covered entities for the purposes of treatment, payment and operations, the greater detail about who can sit down in front of a computer and access data is not consistent across provider organizations. Of particular concern is how to manage information exchange including non-covered entities. In response the Solutions Work Group recommends the following.

Proposed solutions:

3 a. *Standards need to be developed for role based access as defined initially by HIPAA with regard to treatment, payment and operations, and further defined in terms of both covered and non-covered entities and people likely to have access to data.* Specific solutions should attend to the importance of ensuring that information is available where it is needed to provide safe and high quality health care. For example pharmacists need diagnostic information to provide a quality check on prescriptions.

3 b. *The EHR audit trail, documenting by time and date stamp and source all read and write access to PHI, currently required under HIPAA regulations should be reinforced and required under state regulations for all health information exchange.*

3 c. *Standardization of the application of the medical need to know and minimum necessary concepts as currently articulated in state and federal law should include specificity for read and write access in the exchange of PHI.*

3 d. *Automatic reporting of access to one's records should be an option for consumers, with a formal process identified. There should be a standard process for consumer initiated review and/or correction of data to insure integrity of data.*

3 e. *Formulate a model for best practices in security standards that will include a review of all existing security standards. This model should include a data classification schema.*

Domains:
1. User and entity authentication to verify that a person or entity seeking access to electronic personal health information is who they claim to be

2. Information authorization and access controls to allow access to only people or software programs that have been granted access rights to electronic personal health information

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

5. Information protections so that electronic personal health information cannot be improperly modified

Types of HIE:
All
Stakeholders:
All:
Consumers
Government
Hospitals
Long Term Care
Medical Devices
Mental Health
Other Health Care Providers
Payers
Pharmacy
Physicians
Public Health

Stage of Solution:
Role based access and security is in use in many systems, however the roles have not been standardized.

Proposed solution in use by:

Products and systems that use industry best practice models.

Appropriate for a wide range of stakeholders and HIEs:
Especially important for RHIOs as inter-organizational exchange will require agreement on standards.

Barriers to solution:
Dependent upon agreement to a standard.

Barrier: **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.**

Context: The barrier to privacy and security of PHI through health information exchange identified here has to do with the lack of money available to provider organizations to assist in compliance with federal laws and regional practice standards developing in the areas of privacy and security of information exchange. There are both technical and workflow issues included in this barrier which may be addressed through the following solutions.

Proposed solutions:

4 a. *States should take responsibility for developing the basic infrastructure to support health information exchange.* For example in Ohio, the Ohio Department of Development should complete the “last mile” of internet access as defined by the Third Frontier Network.

4 b. *Any publicly funded projects must be standards based including compliance with the Continuity of Care Record (CCR) standard.*

4 c. For publicly funded providers, states should adopt some “pay to play” rules around health information exchange starting with areas such as required vital statistics and disease reporting, state registries, and Medicaid. This would establish some baselines about actual cost of HIPAA privacy and security compliance and provide guidance about cost sharing across various public and private stakeholders.

Domains:
N/A

Types of HIE:
Rural

Stakeholders:
All:
Consumers
Government

Hospitals
Long Term Care
Medical Devices
Mental Health
Other Health Care Providers
Payers
Pharmacy
Physicians
Public Health

Stage of Solution:
Proposed

Proposed solution in use by:
N/A

Appropriate for a wide range of stakeholders and HIEs:
Yes

Barriers to solution:
Funding

Barrier: **5. "Federal and state law requirements that are applicable to mental health and substance abuse records, are stricter than the requirements of HIPAA."**

Context: While there may be components of federal and state law that are "stricter than HIPAA", in the areas of privacy and security with respect to mental health, substance abuse and other diseases such as HIV/AIDS, the barriers identified are more practice based. The concerns raised about electronic exchange of behavioral health data are not directly related to the mode of exchange—paper or electronic—rather to how and when data is exchanged generally. Stakeholders concluded that more public education about the prevalence of mental health and substance abuse, in addition to the treatment options available should take precedence over a continuation of the stigma associated with mental health, substance abuse and other diseases that is perpetuated by the secrecy surrounding PHI, and its exchange electronically. The laws are very clear about restrictions on specific releases of information by the provider outside of a medical need to know and/or duty to warn. However, in response to practice based issues, the Solutions Work Group recommends the following.

Proposed solutions:

5 a. *Current laws and practices that govern the paper release of treatment related information, should be implemented electronically to allow transfer and exchange of data and to track specific patient permissions.*

5 b. *The Continuity of Care Record (CCR), the only current national standard identifying fields for clinical data in an electronic record, should be used as the standard for determining what*

kind of information is routinely exchanged with regard to mental health, substance abuse and other diseases such as HIV/AIDS. This would allow for critical information such as medications to be appropriately available at point of care, but would not require that SOAP or progress notes, or other assessments and evaluations be routinely available. When this additional information is kept in the electronic record, the provider should be able to limit read and write access using role based access.

5 c. As a transitional step between paper and electronic records, a *federal approved emergency release should be adopted that patients routinely provide at the outset of treatment for exchange of information related to mental health, substance abuse and other "sensitive diseases" in case of an emergency.*

5 d. *FERPA and HIPAA regulations should be integrated* to avoid any discrepancies between exchange of data, and concurrent privacy and security protections of data.

5 e. To insure privacy and security of PHI as outlined in HIPAA, s*pecific language should be developed which identifies conditions under which RHIOs or other clearinghouse organizations are routinely designated as covered entities*.

<u>*Domains:*</u>
1. User and entity authentication to verify that a person or entity seeking access to electronic personal health information is who they claim to be

2. Information authorization and access controls to allow access to only people or software programs that have been granted access rights to electronic personal health information

7. Administrative or physical security safeguards required to implement a comprehensive security platform for health IT

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

9. Information use and disclosure policies that arise as health care entities share clinical health information electronically

<u>*Types of HIE:*</u>
All

<u>*Stakeholders:*</u>
All:
Consumers
Government
Hospitals
Long Term Care
Medical Devices
Mental Health

Other Health Care Providers
Payers
Pharmacy
Physicians
Public Health

Stage of Solution:
Proposed

Proposed solution in use by:
N/A

Appropriate for a wide range of stakeholders and HIEs:
Yes

Barriers to solution:
State law and HIPAA interpretation and implementation is not uniform. Stigma about diseases is a public education issue that will require funding.

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

Context: The barrier to the privacy and security of health information exchange identified is somewhat paradoxical—that is if we tip the balance too far on the side of protecting PHI, we run the risk of limiting access to clinical information needed at point of care to insure the highest quality of care. In response the Solutions Work Group recommends the following.

Proposed solutions:

6 a. *Consumer education is needed to articulate the perceived value of health information exchange against the perceived risk of privacy and security breeches in an electronic system.* While the primary concern is around more ready access to information that can be used discriminatorily by employers or insurers, to deny jobs or coverage, there are laws in place to protect people against this kind of discrimination, and that such laws are not well enforced, and often do not provide sufficient remedy to the victim when they have been broken, is not directly related to whether the information is exchanged on paper or electronically, these issues remain in place.

6 b. Because improved quality of care is dependent upon the accurate and comprehensive presentation of health information at the point of care in a timely manner, *increased human oversight, evaluation of data integrity and enforcement of security protections are all recommended.*

Domains:

3. Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises

5. Information protections so that electronic personal health information cannot be improperly modified

Types of HIE:
All

Stakeholders:
All:
Consumers
Government
Hospitals
Long Term Care
Medical Devices
Mental Health
Other Health Care Providers
Payers
Pharmacy
Physicians
Public Health

Stage of Solution:
Proposed

Proposed solution in use by:
N/A

Appropriate for a wide range of stakeholders and HIEs:
Yes

Barriers to solution:
Funding for patient education is not available. Data integrity audits are dependent upon each institution and are not standard practice.

Other identified challenges

Barrier: 7. The release of PHI to parents of an adult child through an explanation of benefit and the potential of the patient foregoing treatment for this reason is a problem. Although this may not fall into the privacy and security arena, it is recommended and that the Department of Insurance should address this issue by examining the exchange of information by payers.

Context:

If this barrier were considered from a patient centric perspective, i.e. the adult child, it would clearly involve privacy and PHI disclosure. However, under the aegis of HIPAA allowing disclosure for payment, the information is disclosed to the policy holder.

Proposed solutions:
The purpose of the explanation of benefits is to audit the provision of care and thus the payment for care. Alternative methods might be developed in an electronic world to perform this function.

Domains:
2. Information authorization and access controls to allow access to only people or software programs that have been granted access rights to electronic personal health information

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

Types of HIE:
All

Stakeholders:
All:
Consumers
Government
Hospitals
Long Term Care
Medical Devices
Mental Health
Other Health Care Providers
Payers
Pharmacy
Physicians
Public Health

Stage of Solution:
Proposed

Proposed solution in use by:
N/A

Appropriate for a wide range of stakeholders and HIEs:
Yes

Barriers to solution:
Consumer concerns have not been articulated.

SUMMARY OF ALL SOLUTIONS:

1 a. *National standards not State standards are the solution.*

1 b. *At the state level, there should be a monitoring body that routinely reviews interpretation, compliance and practice related to the national standards. Planned compliance timelines are needed for smaller institutions and practices.*

1 c. E*lectronic messaging, elements of the clinical record, and transactions are increasingly electronic, national standards at this level should be adopted.*

1 d. As *national standards are implemented, they should be in compliance with the existing standards as defined by HIPAA.*

2 a. *Identify and use a unique identifier for patient identification in the NHIN, with protocols developed for randomized probabilistic matching to routinely verify accuracy of this patient identifier. A risk assessment of the use of any national unique identifier should be included.*

2 b. *In the future, accurate identification of patients should be through biometrics.*

3 a. *Standards need to be developed for role based access as defined initially by HIPAA with regard to treatment, payment and operations, and further defined in terms of both covered and non-covered entities and people likely to have access to data.*

3 b. *The EHR audit trail, documenting by time and date stamp and source all read and write access to PHI, currently required under HIPAA regulations should be reinforced and required under state regulations for all health information exchange.*

3 c. *Standardization of the application of the medical need to know and minimum necessary concepts as currently articulated in state and federal law should include specificity for read and write access in the exchange of PHI.*

3 d. *Automatic reporting of access to one's records should be an option for consumers, with a formal process identified. There should be a standard process for consumer initiated review and/or correction of data to insure integrity of data.*

3 e. *Formulate a model for best practices in security standards that will include a review of all existing security standards. This model should include a data classification schema.*

4 a. *States should take responsibility for developing the basic infrastructure to support health information exchange.*

4 b. *Any publicly funded projects must be standards based including compliance with the Continuity of Care Record (CCR) standard.*

5 a. *Current laws and practices that govern the paper release of treatment related information, should be implemented electronically to allow transfer and exchange of data and to track specific patient permissions.*

5 b. *The Continuity of Care Record, the only current national standard identifying fields for clinical data in an electronic record, should be used as the standard for determining what kind of information is routinely exchanged with regard to mental health, substance abuse and other diseases such as HIV/AIDS.*

5 c. *A federal and state approved emergency release should be adopted that patients routinely provide at the outset of treatment for exchange of information related to mental health, substance abuse and other "sensitive diseases" in case of an emergency.*

5 d. *FERPA and HIPAA regulations should be integrated.*

5 e. S*pecific language should be developed which identifies conditions under which RHIOs or other clearinghouse organizations are routinely designated as covered entities.*

6 a. *Consumer education is needed to articulate the perceived value of health information exchange against the perceived risk of privacy and security breeches in an electronic system.*
6 b. *Increased human oversight, evaluation of data integrity and enforcement of security protections are all recommended.*

Organization of Solutions:

A. Solutions affecting variations in organization business practices and policies (but not affecting state laws)
1 b. *At the state level, there should be a monitoring body that routinely reviews interpretation, compliance and practice related to the national standards. Planned compliance timelines are needed for smaller institutions and practices.*
4 a. *States should take responsibility for developing the basic infrastructure to support health information exchange.*
4 b. *Any publicly funded projects must be standards based including compliance with the Continuity of Care Record (CCR) standard.*
6 a. *Consumer education is needed to articulate the perceived value of health information exchange against the perceived risk of privacy and security breeches in an electronic system.*
6 b. *Increased human oversight, evaluation of data integrity and enforcement of security protections are all recommended.*

B Solutions affecting state laws/regulations
5 a. *Current laws and practices that govern the paper release of treatment related information, should be implemented electronically to allow transfer and exchange of data and to track specific patient permissions.*
5 b. *The Continuity of Care Record, the only current national standard identifying fields for clinical data in an electronic record, should be used as the standard for determining what kind of information is routinely exchanged with regard to mental health, substance abuse and other diseases such as HIV/AIDS.*
5 c. *A federal and state approved emergency release should be adopted that patients routinely provide at the outset of treatment for exchange of information related to mental health, substance abuse and other "sensitive diseases" in case of an emergency.*

C. Solutions affecting federal laws/regulations
1 a. *National standards not State standards are the solution.*
1 c. E*lectronic messaging, elements of the clinical record, and transactions are increasingly electronic, national standards at this level should be adopted.*
1 d. As *national standards are implemented, they should be in compliance with the existing standards as defined by HIPAA.*
2 a. *Identify and use a unique identifier for patient identification in the NHIN, with protocols developed for randomized probabilistic matching to routinely verify accuracy of this patient identifier. A risk assessment of the use of any national unique identifier should be included.*
2 b. *In the future, accurate identification of patients should be through the use of biometrics.*

3 a. *Standards need to be developed for role based access as defined initially by HIPAA with regard to treatment, payment and operations, and further defined in terms of both covered and non-covered entities and people likely to have access to data.*
3 b. *The EHR audit trail, documenting by time and date stamp and source all read and write access to PHI, currently required under HIPAA regulations should be reinforced and required under state regulations for all health information exchange*.
3 c. *Standardization of the application of the medical need to know and minimum necessary concepts as currently articulated in state and federal law should include specificity for read and write access in the exchange of PHI.*
3 d. *Automatic reporting of access to one's records should be an option for consumers, with a formal process identified. There should be a standard process for consumer review and/or correction of data to insure integrity of data.*
3 e. Formulate a model for best practices in security standards that will include a review of all existing security standards. This model should include a data classification schema.
5 a. *Current laws and practices that govern the paper release of treatment related information, should be implemented electronically to allow transfer and exchange of data and to track specific patient permissions.*
5 b. *The Continuity of Care Record, the only current national standard identifying fields for clinical data in an electronic record, should be used as the standard for determining what kind of information is routinely exchanged with regard to mental health, substance abuse and other diseases such as HIV/AIDS.*
5 c. *A federal and state approved emergency release should be adopted that patients routinely provide at the outset of treatment for exchange of information related to mental health, substance abuse and other "sensitive diseases" in case of an emergency.*
5 d. *FERPA and HIPAA regulations should be integrated.*
5 e. S*pecific language should be developed which identifies conditions under which RHIOs or other clearinghouse organizations are routinely designated as covered entities*.

D. Solutions affecting Interstate Health Information Exchanges

None

Section 5 - National-level Recommendations

National standards are pivotal to the effective exchange of health information across organizations, states and territories. The states' responsibilities in health information exchange hinge upon the development and implementation of those standards. The recommendation that Ohio puts forward is to require the use of the Continuity of Care Record standard as the first adoption target. Multiple federal laws including FERPA, HIPAA, mental health and substance abuse law must be harmonized and guidance must be issued about the status of RHIOs as covered entities. Each state cannot provide solutions to these national issues, nor should they be asked to as such solutions might result in 50+ variants, one from each state or territory.

Appendix A
Solutions Working Group Members

LAST NAME	FIRST NAME	ORGANIZATION	CITY	STATE
Alt	Doug	State IT Policy Manager, Statewide IT Policy, Investment and Governance Division Office of Information Technology	Columbus	OH
Bartone	Dominic	Hocks Vandalia Pharmacy, Dayton	Tipp City	OH
Bateson	Lisa	Anthem	Columbus	OH
Bertka	Kenneth	Medical Director of Information and Process Services, Mercy Health Partners	Toledo	OH
Biddlestone	Elayne	Academy of Medicine of Cleveland	Cleveland	OH
Blackburn	Sally	North Dayton Community	Dayton	OH
Bohlander	Tricia	Senior Analyst, LifeMasters of Self Care, Inc.	Columbus	OH
Boyd	Ernest	Ohio Pharmacist Association	Columbus	OH
Brown	Nancy	Priority Board, Neighborhood Association	Dayton	OH
Brown	Ruth	Heartland Information Services	Toledo	OH
Callahan	Walter	Leadership Management Committee (LMC)	Columbus	OH
Cauley	Kate	Center for Healthy Communities WSU Boonshoft School of Medicine	Dayton	OH
Crimmins	Mary	Center for Healthy Communities WSU Boonshoft School of Medicine	Dayton	OH
Davis	Martha	Data Systems Specislist, St. Vincent Mercy Medical Center/Mercy Children's Hospital	Toledo	OH
Donley	Alana	Leadership Management Committee (LMC)	Columbus	OH
Fligor	Larry	Chief Technology Officer, Ritzman Pharmacies	Akron	OH
Fredette	Beth	Children's Medical Center	Dayton	OH
Frick	Shawn	Ohio Primary Care Association	Columbus	OH
Grant	Janet	CareSource	Dayton	OH
Hall	Ronald	Consultant	Columbus	OH
Hayes	Bill	Health Policy Institute of Ohio	Columbus	OH
Hotte	Bruce	Leadership Management Committee (LMC)	Columbus	OH
Hunt	Cynthia	Leadership Management Committee (LMC)	Columbus	OH
Kapp	Jeffrey	Jones Day	Columbus	OH
Keiser	Kim	Ohio Hospital Association	Columbus	OH
Kreitel	Ken	Leadership Management Committee (LMC)	Columbus	OH
LeRoy	Gary	East Dayton Health Center, Ohio Academy of Family Physicians, Dayton	Dayton	OH
Liston	Kim	Leadership Management Committee (LMC)	Columbus	OH
Mares	Aileen	Combined Health District of Montgomery County, Health Commissioner	Dayton	OH
McAndrew	James	Leadership Management Committee (LMC)	Columbus	OH
McLean	Denny	Regional Information Security Administrator Mercy Health Partners	Toledo	OH
Morgan	Nyle	Kettering Medical Center Network CIO	Miamisburg	OH
Paschall	Anne	ODMH	Columbus	OH
Patterson	Alonzo	PriMed Physicians Group in Dayton	Dayton	OH
Penrod	Burger	Leadership Management Committee (LMC)	Columbus	OH
Ranbom	Lorin	Assistant Deputy Director, Ohio Department of Job and Family Services	Columbus	OH
Reed	Heather	Ohio Department of Health	Columbus	OH
Rowe	Phil	Leadership Management Committee (LMC)	Columbus	OH
Smiles	Terri-Lynne B.	Collis Smiles & Collis	Columbus	OH
Smith	Megan	Ohio Academy of Family Physicians, Dayton	Columbus	OH
Solano-McGuire	Sandra	MD MS Office of Ohio Health Plans ODJFS	Columbus	OH
Speed	Becky	AHIMA, OHIMA, HIM Consultant, RHIA	Columbus	OH
Wayne	Matthew	Eliza Jennings Senior Care Network	Olmstead Twp	OH
White	Margie	Columbus Colony Elderly Care	Westerville	OH
Wolf	Eve	PhD, psychologist, MC Psychological Association, Dayton	Dayton	OH