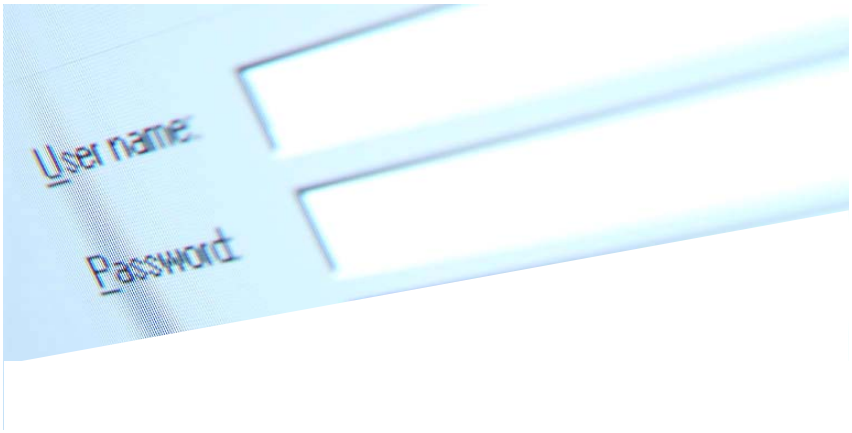
Privacy and Security Solutions for Interoperable Health Information Exchange

North Carolina HISPC

Final Assessment of Variation and Analysis of Solutions



Submitted by:
Holt Anderson, Executive Director
NCHICA
3200 Chapel Hill/Nelson Blvd.,
Suite 200, Cape Fear Building
PO Box 13048
Research Triangle Park, NC 27709-3048

Submitted to:
Linda Dimitropoulos, Project Director
Privacy and Security Solutions for
Interoperable Health Information Exchange
RTI International
P. O. Box 12194
3040 Cornwallis Road
Research Triangle Park, NC 27709-2194

March 30, 2007

Subcontract No. 37-321-0209825
RTI Project No. 9825

NCHICA

NC HISPC
North Carolina Health Information Security and Privacy Collaboration

RTI INTERNATIONAL

What is NCHICA, RTI, AHRQ?

About the North Carolina Healthcare Information and Communications Alliance (NCHICA)

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) is a nonprofit consortium of over 200 organizations dedicated to improving healthcare by accelerating the adoption of information technology. NCHICA members represent the diverse sectors of the healthcare community, including providers, payers, vendors, professional societies, and law firms. To see a list of members, click here.

NCHICA's role is to act as a neutral forum to bring together the many sectors of the healthcare industry. Together we can address how best to accelerate the adoption of IT in healthcare by considering clinical needs, policy questions and technology issues.

About the Agency for Healthcare Research and Quality

The Agency for Healthcare Research and Quality (AHRQ) is the nation's lead Federal agency for research on health care quality, costs, outcomes, and patient safety. AHRQ is the health services research arm of the U.S. Department of Health and Human Services (HHS). Health services research examines how people get access to health care, how much care costs, and what happens to patients as a result of this care. AHRQ supports improvements in health, develops strategies to strengthen quality measurement and improvement, and identifies strategies to improve health care access, foster appropriate use, and reduce unnecessary expenditures. AHRQ gives information and technical assistance to State and local policymakers through user-driven workshops on topics that include improving care delivered to children served by state agencies and developing strategies to reduce health disparities.

About RTI International

RTI International is one of the world's leading research institutes, dedicated to improving the human condition by turning knowledge into practice. With projects in more than 40 countries and a staff of more than 2,600, RTI offers innovative research and technical solutions to governments and businesses worldwide in the areas of health and pharmaceuticals, education and training, surveys and statistics, advanced technology, democratic governance, economic and social development, energy, and the environment. RTI combines the skills and expertise of staff to provide unique programs and capabilities within a wide range of technical and social sciences. RTI personnel form a research organization of four major groups -- Social and Statistical Sciences, Science and Engineering, International Development, and RTI Health Solutions – as well as its administrative organization. From these groups, RTI can form a wide variety of multidisciplinary teams focused on unique, leading-edge research and development projects.

Table of Contents

Disclaimer

While the information and recommendations contained in the North Carolina Health Information Security and Privacy Collaboration (NC HISPC) documents and website have been compiled from sources believed to be reliable, NC HISPC makes no guarantee as to, and assumes no responsibility for, the accuracy, sufficiency, or completeness of such information or recommendations.

Links made from the reference documents submitted shall not represent an endorsement by the State of North Carolina, NC HISPC, or NCHICA or by its members, board of directors, committees, or staff. The views and opinions of authors expressed within the documents and website do not necessarily state or reflect those of the State of North Carolina, NC HISPC, or NCHICA or its members, board of directors, committees, or staff, and they may not be used for endorsement purposes.

The information provided is not intended to constitute an "authoritative statement" under the State of North Carolina’s policies, general statutes, and regulations.

Acknowledgements

NCHICA would like to acknowledge the following members of the North Carolina Health Information Privacy and Security Collaboration team for their contributions to the North Carolina HISPC Final Assessment of Variation and Analysis of Solutions Report:

Project Director
Angie M. Santiago,
TM Floyd & Company, Inc.

NC HISPC Co-Chairs
David Kirby, Kirby Information Management Consulting
Patricia A. Markus, Smith Moore LLP
James Murphy, NC DHHS MMIS
Mike Voltero, BCBSNC
Roy H. Wyman, Jr., Williams Mullen Maupin Taylor

Contributors
Sherrie Cannoy, UNC Greensboro
Vincent Carrasco, MD, Radarfind Co.
Cathy Chapman, BCBSNC
Joe Cimbala, DHHS-DMH/DD/SAS-RRM/IS
Kathy Goliszek, Forsyth Medical Group – Novant Health
Christine Jacob, BCBSNC
Heidi Jurgens, BCBSNC
Donald Sweezy, Duke University Health System
Andrew Weniger, eHealth Initiative
Katherine White, NC Office of IT Services
Judy Beach, Quintiles Transnational Corp.
Shannon Buckner, BCBSNC
Jackie Chapman-Pointer, BCBSNC
John Doyle, LabCorp
Alicia Gilleskie, Misys
Sissy Holloman, UNC Hospitals
Randy Sermons, Randall E Sermons, Sanderson Law
Steve Stonecypher, LabCorp
Variations Work Group
Solutions Work Group
Legal Work Group

NC HISPC Steering Committee
Holt Anderson, NCHICA
Phil Telfer, NC Governor's Office
Linda Attarian, NC DHHS Div. of Medical Assistance
Wesley G. Byerly, Pharm.D., WFUBMC
Fred Eckel, NC Association of Pharmacists
Jean T. Foster, NCHIMA / Pitt County Memorial Hosp,
Donald E. Horton, Jr., LabCorp
Eileen Kohlenberg, Ph.D., NC Nurses Association
Mark Holmes, PH.D., NC Institute of Medicine
Linwood Jones, NC Hospital Association
Patricia MacTaggart, Health Management Association
Lawrence Muhlbaier, Ph.D., Duke Uniiv. Health System
David Potenziani, M.D., UNC School of Public Health
Melanie Phelps, NC Medical Society
N. King Prather, BCBSNC
Morgan Tackett, BCBSNC

Editor
Diana Gildea, Project Coordinator

Executive Summary

Background

In April 2004, President George W. Bush articulated his vision for the future of health care in the United States by an Executive Order that authorized the Secretary of the Department of Health and Human Services (HHS), Michael Leavitt, to establish the Office of the National Coordinator for Health Information Technology (ONC) which provides leadership for the development and nationwide implementation of an interoperable health information technology infrastructure to improve the quality and efficiency of health care and the ability of consumers to manage their care and safety.

In October 2005, ONC and the Agency for Healthcare Research and Quality (AHRQ) awarded the Privacy and Security Solutions for Interoperable Health Information Exchange contract to RTI International. RTI, in collaboration with the National Governors Association (NGA) Center for Best Practices, formed the Health Information Security and Privacy Collaboration (HISPC) project and invited the states and territories to submit proposals to participate in the project. The HISPC project was designed to examine privacy and security laws and business practices that affect the ability of every state and territory to exchange electronic health information within itself and among each other.

NCHICA submitted a proposal and in April 2006 was awarded the contract to represent North Carolina. Since the project's commencement, teams of healthcare stakeholders worked collaboratively through a process of consensus to identify, assess, and develop plans to address variations in organization-level business policies and state laws that affect privacy and security practices that may pose challenges to health information exchange.

Purpose

The purposes of the North Carolina Health Information Privacy and Security Collaboration (HISPC) project are to address variations in organization-level business policies and state laws that affect privacy and security practices which, in turn, may pose challenges to interoperable health information exchange; to recommend solutions and implementation plans to reduce or eliminate those challenges; and to increase the level of expertise in and compliance with privacy protections within the healthcare community.

NC HISPC's goals are to:

1. identify current healthcare practices and challenges regarding the release and exchange of health information,
2. develop consensus-based solutions for interoperable electronic health information exchange (HIE) that protect the privacy and security of health information, and
3. recommend high-level plans to implement recommended solutions.

The NC HISPC project recommends policy, technological, and legal solutions to the barriers or obstacles identified in the Assessment of Variations Report. In addition to identifying solutions, the Report also documents, for each potential solution, the HIE context, privacy and security domains affected, involved stakeholders, HIE barriers that are addressed, and each solution's current stage of development.

Workgroup Composition

The Variations, Legal, Solutions, and Implementation Workgroups are comprised of attorneys; practice managers; researchers; clinicians; and professionals in public health policy, health information management, and information security specializing in health information privacy and security who represent healthcare stakeholders such as consumers, health plans, professional organizations, healthcare facilities, laboratories, healthcare software vendors, and public health agencies.

The Variations Workgroup (VWG) conducted individual and group assessments to document the stakeholders' current practices if they were presented with each of the 18 healthcare scenarios provided by RTI. The VWG was charged with collecting the business practice data and identifying potential barriers to exchanging health information. The VWG was co-chaired by Jim Murphy from the NC Department of Health and Human Services Office of Medicaid Management Information Systems (NC DHHS MMIS), Mike Voltero, General Counsel to Blue Cross Blue Shield of North Carolina, and Roy H. Wyman, Jr., a partner at Maupin Taylor Williams Mullen.

The Legal Workgroup (LWG) analyzed the business practices provided by the VWG and identified legal sources of the barriers to exchanging health information. The LWG was chaired by Patricia A. Markus, a partner at Smith Moore LLP. The LWG was comprised of members representing the following stakeholders: Blue Cross Blue Shield of North Carolina, CareSpark, FirstHealth of the Carolinas, LabCorp, Williams Mullen Maupin Taylor, NC DHHS Department of Medical Assistance, NC Hospital Association, NC Medical Society, Pitt County Memorial Hospital, NC Health Information Management Association, Quintiles Transnational, MISYS, NC Office of Information Technology Services, and UNC Hospitals.

The Solutions and Implementation Plan Workgroups (SWG and IPWG) reviewed the data collected from the VWG and developed solutions and implementation plans to reduce or remove the identified barriers. The SWG and IPWG were chaired by Dave Kirby, President of Kirby Information Management Consulting. The SWG and IPWG were comprised of members representing the following healthcare stakeholders: Blue Cross Blue Shield of North Carolina, Duke University Health System, eHealth Initiative, E-Tech Security Pro, NC DHHS Office of Medicaid Management Information Services, NC Department of Mental Health and Substance Abuse, Novant Health, and Radarfind.

With the exception of the PMO, all project participants have voluntarily contributed their time and expertise to this project.

Methodology

RTI International provided NC HISPC with 18 scenarios to analyze along nine domains of privacy and security. Each scenario represented a business practice or health care scenario that required the exchange of health information between different entities within North Carolina and other states. NC HISPC grouped the 18 scenarios into four sub-group work clusters based on the type of stakeholders interviewed, the legal sources for the barriers, the security domains relevant to the scenarios, and the field of expertise of each professional participant.

The scenarios' four sub-group work clusters are:

NC HISPC Scenario Sub-Group Work Clusters	
Sub-group 1: Patient Care Scenarios 1. Patient Care A (Emergency Transfer) 2. Patient Care B (Substance Abuse) 3. Patient Care C (Access Security) 4. Patient Care D (HIV and Genetics)	Sub-group 2: Payer Scenarios 5. Payment (EHR Access) 9. Pharmacy Benefit A (Mail Order) 10. Pharmacy Benefit B (Claims Savings)
Sub-group 3: Secondary Use Scenarios 6. RHIO (Data Access) 7. Research (Data Usage) 8. Law Enforcement (Test Results) 11. Operations and Marketing A (Rehab Center) 12. Operations and Marketing B (Birthing PHI) 14. Employment Information (Return to Work	Sub-group 4: Government, Public Health & Safety Scenarios 13. Bioterrorism Event (Anthrax Spread) 15. Public Health A (Active TB Carrier) 16. Public Health B (Newborn Screening) 17. Public Health C (Homeless Shelters) 18. Health Oversight (Legal Compliance)

The PMO developed a facilitator training program to ensure that interviewees were comfortable sharing the policies and practices of their organization during the assessment interviews. The

training program elements included confidentiality reassurance, guidance to maintain objectivity, suggestions for how to focus discussions on the presented scenarios and work session questions, and re-capping information for the recorders. Each VWG session was facilitated and recorded by one or more of the project Co-Chairs, the Project Manager, and the Project Coordinator.

In preparation for the assessment sessions, the Co-Chairs formulated seven questions to focus on the "who, what, how, and why" of the organization's business practices around sharing information that correlated to the assessment tool fields. These are the questions each interviewee was asked:

1. What is your stakeholder type?
2. What is your current business practice if presented with this type of scenario?
3. Why is that your current business practice?
4. Does this business practice aid the exchange of health information with other entities?
5. Does this business practice present a barrier to exchanging health information?
6. Is this barrier appropriate to safeguard the information?
    a. Why is it appropriate?
    b. If not, could you recommend an alternate solution to removing this barrier?
7. How is this particular business practice affected in a manual or electronic environment?

These seven questions guided the Workgroups as they documented the practices shared by the stakeholders, identified barriers and their legal sources, and developed solutions and implementation plans to reduce or eliminate the barriers to exchanging electronic health information.

The following steps were taken to identify the legal drivers of the information-sharing business practices:

1. The LWG reviewed the scenarios.
2. The LWG researched the NC and federal laws relevant to the type of health information exchange addressed in the scenario.
3. Then the LWG was given access to the results of the assessment sessions. The group reviewed the interviewees' current practices and policies.
4. The LWG identified the gaps between the relevant laws and the current understanding and application of those laws by the various health organizations.
5. The LWG recommended solutions to the legal barriers presented. The group also advised the SWG on proposed policy solutions which either may pose a liability risk to stakeholders or may conflict with state or federal law.

The Solutions Work Group (SWG) Chair, Dave Kirby, developed a work plan that included weekly goals to allow members to understand first the problems and issues, and then to formulate candidate solution outlines, followed by an opportunity to add commentary to those solution outlines that then would be analyzed and commented upon by other project participants. This last element took the form of written sub-group reports. The work plan allowed each subgroup to work simultaneously. This design feature reduced the risk of missing the large project milestones because of a single group's delay. The plan called for the sub-groups to vet the various solutions and was structured to allow every viewpoint to be represented in the interim and final reports, along with group views of the applicability of each solution offered. This part of the plan anticipated an environment in which there was sufficient risk to each barrier and sufficient urgency in finding solutions, and that each offered solution would be pressed forward in some venue in NC at least to the point that it is field-tested. The Project Manager correlated and consolidated the various inputs and developed the report.

The HISPC Domains of Privacy and Security

RTI supplied the NC HISPC team with a set of domains to consider as the SWG and LWG considered solutions. This set of domains is derived from standard information security principles.

Domains 1 - 6 are relevant to organizations that have implemented electronic health information systems. Due to the limited amount of implemented technology among the interviewees, most of the barriers that were identified centered around domains 7 – 9.

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

Summary of Relevant Findings

The VWG and LWG analyzed the responses from the stakeholders and identified policy, legal, and technological barriers that prevented or delayed the exchange of health information. While this section of the report contains a general overview of the barriers to exchange that were identified by the VWG and LWG, detailed information is contained within the report.

BR_1. Range within organizations of misinterpretation and/or misapplication of laws or regulation

Interviewees consistently shared that unless they were required to share the information, they would rather "protect" it for fear of being held liable for breaching an individual's right to privacy. The VWG, LWG, and SWG found that the majority of the misinterpretation or misapplication of laws, regulations, or organizational policies stemmed from a lack of awareness that the law, regulation, or policy existed, or from a lack of training that was meaningful to the organization or individual.

BR_2. Lack of business incentives to exchange information

Clinicians who were interviewed feared that engaging in an interoperable health information exchange such as a RHIO could cause them to lose patients to other providers. They also were interested in the benefits of what EHRs may bring but weren't sure how such large monetary investments in technology could benefit their patients or their practices. The SWG believes that the lack of health information technology adoption and exchange are due to providers' perception that HIT lacks value, to the lack of funding to implement such technology, and to a lack of incentives for sharing information among other entities.

BR_3. Lack of policy standardization across entities

The interviewees and members of the LWG and SWG observed an overall lack of policy standards within their own organizations and industry-wide. Consents and authorizations to treat patients and to release patient information vary from entity to entity. Differing legal and political philosophies cause differing approaches to the application of laws and regulations, resulting in differing information-sharing practices among health care stakeholders.

BR_4. Lack of security standardization across entities

A consensus among the VWG, LWG, and SWG concur that the HIPAA Privacy and Security Rules laid the foundation for entities to develop privacy and security programs. However, if the goal is to implement an interoperable health information network in order to securely exchange

electronic health information, then specific, formal security standards should be identified and adopted by the healthcare community.

BR_5. Lack of interoperability between processes and technology
The healthcare system is fragmented. Before technology is implemented, a review of the industry's healthcare processes should be undertaken to identify where the breakdowns in interoperability occur and whether the appropriate remedies for each breakdown are ones of process or technology.

BR_6. Lack of workable technology
The adoption of effective health information technology is critical to an interoperable nationwide health information network.

BR_7. Conflicting or outdated federal or state laws or regulations
Current privacy laws were appropriately implemented to protect the confidentiality of information. As electronic information exchange increases, however, laws focusing on the confidentiality, protection, and disposal of information contained in paper format should be reviewed and updated to reflect the new medium of exchange.

Consumer Empowerment Barriers
The following barriers were not derived from stakeholder responses. They have been identified by the SWG and LWG in response to the ONC's objectives of ensuring that consumer concerns are identified and represented as the development and implementation of the Nationwide Health Information Network (NHIN) ensues.

BR_8a. Lack of consumer understanding or awareness of the benefits of HIT leads to a lack of consumer input into the policy and technology that support health information exchange
To ensure usability, systems designers should engage consumers and seek regular input on how consumers can use health information technology and exchange to improve their health.

BR_8b. Lack of definition of consumer empowerment and lack of methodology for including consumers in policy and systems design
Clarifying the term "consumer empowerment" in relation to the ONC's strategy would assist policymakers and technology experts in developing policy and technology that empowers and improves the lives of consumers. If consumer empowerment includes consumers' ability to manage the access to their health information, then application software would be required to include such features.

Sub-Group 1: Patient Care Direct Treatment Scenarios

1. Patient Care A (Emergency Transfer)
2. Patient Care B (Substance Abuse)
3. Patient Care C (Access Security)
4. Patient Care D (HIV and Genetics)

Sub-Group 1 Stakeholders
Twenty-nine respondents participated in the assessment sessions for Sub-Group 1, the patient care scenarios. The respondents included physician groups, clinicians, hospital health information managers (HIM) and nursing staff, researchers, hospital privacy officials, and health law attorneys (who responded on behalf of their hospital clients or were familiar with hospital operational issues).

The stakeholders reviewed the scenarios and described their organizations' practices with regard to each scenario.

An overview of the barriers identified by the VWG and LWG is below:

Stakeholders' Responses - Barriers Sub-Group 1: Patient Care Scenarios				
Barriers	SC - 1	SC – 2	SC – 3	SC - 4
BR_1. Misinterpretation of laws		29		
BR_2. Lack of business incentives				
BR_3. Lack of policy				
BR_4. Lack of security		29		
BR_5. Lack of interoperability	29			
BR_6. Lack of technology	29			
BR_7. Conflicting laws		29	29	29

Privacy and Security Domains Addressed

Domains Represented Sub-Group 1: Patient Care				
Domains	Scenario 1	Scenario 2	Scenario 3	Scenario 4
1. Authentication	X		X	
2. Authorization	X	X	X	X
3. Identity Matching	X	X	X	X
4. Transmission	X	X	X	X
5. Integrity			X	
6. Event Audit			X	X
7. Safeguards			X	
8. Data classification	X			X
9. Policies	X	X	X	X

Sub-Group 2: Payment Scenarios

5. Payment (EHR Access)
9. Pharmacy Benefit A (Mail Order)
10. Pharmacy Benefit B (Claims Savings)

Sub-Group 2 Stakeholders

Nine individuals responded to scenario 5. They included staff members from the payer community who specialize in case management, as well as health and corporate law. Respondents to scenario 7 included HIPAA privacy officials, physician group administrators, health information professionals, clinicians, and research professionals. No pharmacy benefit managers responded to the invitation to participate in the assessment regarding scenarios 9 and 10.

The stakeholders reviewed the scenarios and described their organizations' practices with regard to each scenario.
An overview of the barriers identified by the VWG and LWG is below:

Stakeholders' Responses - Barriers Sub-Group 2: Payer / PBM Scenarios			
Barriers	SC – 5	SC – 9	SC - 10
BR_1. Misinterpretation of laws			
BR_2. Lack of business incentives			
BR_3. Lack of policy			
BR_4. Lack of security			
BR_5. Lack of interoperability			
BR_6. Lack of technology	9		
BR_7. Conflicting laws	9		

Privacy and Security Domains Addressed

Domains Represented

Sub-Group 2: Payer / PBM				
Domains	Scenario 5	Scenario 7	Scenario 9	Scenario 10
1. Authentication	X			
2. Authorization	X			X
3. Identity Matching	X		X	
4. Transmission	X		X	
5. Integrity		X		X
6. Event Audit	X	X		
7. Safeguards				
8. Data classification		X	X	
9. Policies	X	X	X	X

Sub-Group 3: Secondary Use Scenarios

Sub-Group 3 scenarios were based on the uses and disclosures of health information for the purposes of conducting healthcare operations, marketing, or work-related activities which have no impact on direct patient care.

6. RHIO (Data Access)
7. Research (Data Usage)
8. Law Enforcement (Test Results)
11. Operations and Marketing A (Rehab Center)
12. Operations and Marketing B (Birthing PHI)
14. Employment Information (Return to Work)

Sub-Group 3 Stakeholders

The 27 respondents for scenario 6 included individuals representing clinicians, hospitals, health plans, public health agencies, laboratories, pharmacies, professional associations, and academic medical centers. The 32 respondents for scenario 8 included individuals representing clinicians, hospitals, payers, public health agencies, laboratories, pharmacies, law enforcement, professional associations, academic medical centers, county government, and the legal community. The 5 respondents for scenarios 11 and 12 (Group 3 Healthcare Marketing and Operations) included marketing professionals that specialize in hospital wellness programs from the hospital, payer, and disease management communities. The 26 respondents for scenario 14 (Employee Health Information) included human resources professionals and employees from self-insured employers, payers, academic medical centers, hospitals, and group practice administrators.

The stakeholders reviewed the scenarios and described their organizations' practices with regard to each scenario.

An overview of the barriers identified by the VWG and LWG is below:

Stakeholders' Responses - Barriers Sub-Group 3: Secondary Use of Health Information Scenarios						
Proposed Solutions	SC - 6	SC – 7	SC – 8	SC – 11	SC – 12	SC - 14
BR_1. Misinterpretation of laws				5	5	26
BR_2. Lack of business incentives		1				
BR_3. Lack of policy	27					
BR_4. Lack of security	27					
BR_5. Lack of interoperability		1				
BR_6. Lack of technology		1				26
BR_7. Conflicting laws	27		32			26

Sub-Group 4: Government, Public Health & Safety Scenarios

13. Bioterrorism Event (Anthrax Spread)
15. Public Health A (Active TB Carrier)
16. Public Health B (Newborn Screening)
17. Public Health C (Homeless Shelters)
18. Health Oversight (Legal Compliance)

Sub-Group 4 Stakeholders

Respondents to scenarios 13, 15-18 (Group 4 Public Health and State Government) included NC state government employees representing public health agencies, substance abuse, mental health, emergency management, laboratories, hospitals, clinicians, medical and public health schools, health information management, disaster and homeland security professionals. There were no participants from drug treatment centers or homeless shelters.

The stakeholders reviewed the scenarios and described their organizations' practices with regard to each scenario.

An overview of the barriers identified by the VWG and LWG is below:

Stakeholders' Responses - Barriers Sub-Group 4: State Govt. & Public Health Scenarios					
Proposed Solutions	SC – 13	SC – 15	SC – 16	SC – 17	SC – 18
BR_1. Misinterpretation of laws					
BR_2. Lack of business incentives					
BR_3. Lack of policy	19				
BR_4. Lack of security					
BR_5. Lack of interoperability	19	11			8
BR_6. Lack of technology		11			8
BR_7. Conflicting laws			12	14	

Privacy and Security Domains Addressed

Domains Represented Sub-Group 4: State Govt. & Public Health					
Domains	Scenario 13	Scenario 15	Scenario 16	Scenario 17	Scenario 18
1. Authentication			X		X
2. Authorization	X	X	X	X	X
3. Identity Matching	X	X	X	X	X
4. Transmission		X	X	X	X
5. Integrity	X	X	X		X
6. Event Audit	X			X	X
7. Safeguards					X
8. Data classification	X	X	X	X	X
9. Policies	X	X	X	X	X

Summary of Solutions

The VWG, LWG, and SWG analyzed the barriers to information exchange and proposed solutions to reduce or eliminate barriers that delay or prevent stakeholders from exchanging health information with each other. The solutions are organized by characterizing the scope of the practice of information exchange to which each solution would apply, along with organizations that indicate the traits of various solutions related to historical issues of electronic health data exchange.

This section of the report includes a list of the proposed solutions being considered among the HISPC project participants. Each proposed solution contains further detail on the barrier that it addresses; the rationale for this particular proposed solution; an alternate solution, if applicable; to whom the proposed solution applies; and potential barriers to implementing the proposed solution. The Implementation Plan Report will contain detailed information on the anticipated length of implementation, potential resources for, and steps to implement each solution.

These proposed solutions are not ranked in any particular order of priority:

SOL_1. Establish a pilot project with adequate funding to explore the concept of the Person-Oriented HIE.
SOL_2. Implement policy standards, such as model policy and legislation, to address the complexity and ambiguity surrounding the release of information.
SOL_2a. Implement security standards to address the complexity and ambiguity surrounding the safeguarding of health information.

SOL_3. Implement sound business models to incentivize potential information sharing partners to participate in community-based health information exchange.
SOL_4. Encourage greater collaboration between policy makers and subject matter and technical experts to adopt HIE requirements.
SOL_5. Explore the dependencies between the business processes and their technical components for the purpose of interoperability.
SOL_6. Address the misinterpretation of laws or regulations by obtaining clarification and developing public and private awareness programs.
SOL_7. Amend conflicting federal or state laws.
SOL_8. Develop programs to increase awareness about the risks, benefits, and effects of health information technology among a cross-section of consumers.

Conclusions and Next Steps

The HISPC project has convened a core group of North Carolina consumers and health care professionals from varying segments of the health care system. The discussions within the VWG, LWG, SWG, Steering Committee, and Consumer Advisory Council meetings have generated interest in further exploring the identified barriers and implementing the proposed solutions. The Implementation Plan Report will propose high-level steps for interested stakeholders to consider as they plan for the implementation of the proposed solutions.

The implementation challenge for the North Carolina stakeholders is that there is no executive-level mandate or financial sponsorship to spur implementation of the proposed solutions at this time. Therefore, the next steps for the North Carolina stakeholders will be to:

1. Raise awareness about the expected benefits of adopting health information technology
2. Develop programs that foster the growth of HIT thought leadership
3. Educate and engage the General Assembly in the promotion of HIT
4. Cultivate the Consumer Advisory Council

To participate in the continuing efforts or to view more information on the NC HISPC efforts, please see the NCHICA site at: http://www.nchica.org/NCHISPC/intro.htm

HISPC Background and Purpose

Historical Background

In April 2004, President George W. Bush articulated his vision for the future of health care in the United States by an Executive Order that authorized the Secretary of the Department of Health and Human Services (HHS), Michael Leavitt, to establish the Office of the National Coordinator for Health Information Technology (ONC) which provides leadership for the development and nationwide implementation of an interoperable health information technology infrastructure to improve the quality and efficiency of health care and the ability of consumers to manage their care and safety. The National Coordinator for Health IT is the chief advisor to the Secretary of HHS on the actions needed to meet the President's call for widespread availability of secure, interoperable health information technology.

In October 2005, ONC and the Agency for Healthcare Research and Quality (AHRQ) awarded the Privacy and Security Solutions for Interoperable Health Information Exchange contract to RTI International. RTI, in collaboration with the National Governors Association (NGA) Center for Best Practices, formed the Health Information Security and Privacy Collaboration (HISPC) project and invited the states and territories to submit proposals to participate in the project. The HISPC project was designed to examine privacy and security laws and business practices that affect the ability of every state and territory to exchange electronic health information within itself and among each other.

NCHICA submitted a proposal and in April 2006 was awarded the contract to represent North Carolina. Since the project's commencement, teams of healthcare stakeholders worked collaboratively through a process of consensus to identify, assess, and develop plans to address variations in organization-level business policies and state laws that affect privacy and security practices that may pose challenges to health information exchange.

Health Information Initiatives within North Carolina

Several strategic health information technology (HIT) initiatives have been undertaken or currently exist in North Carolina. A collaborative project with IBM, under a contract with the Office of the National Coordinator for Health Information Technology, developed a Nationwide Health Information Network (NHIN) architecture prototype. At the NHIN forum in January 2007, communities in the Research Triangle, NC and Rockingham County, NC/Danville, VA areas successfully demonstrated an interoperable NHIN that seamlessly exchanged health information consisting of patients' demographic information, clinical history, medications, and laboratory results.

The North Carolina Healthcare Quality Initiative (NCHQI) is a multiple-stakeholder project designed to automate medication, laboratory, and radiology data. The first phase of the project involves providing a list of patient medications to the patient's health care provider at the point of contact, so that the provider can evaluate possible drug-to-drug interactions and prescribe correct dosages. The second phase of the project contemplates the electronic exchange of laboratory and radiology data to further improve care and save time. Consumers will receive all of the above-noted benefits of the project while simultaneously receiving assurance that the privacy and security of their health information is being maintained. Later phases encourage a broader use of electronic health records and personal health records.

Another ongoing initiative is the Automated Adverse Drug Events Detection and Intervention project, underway at Duke University, which establishes an automated surveillance system for detecting, reporting, intervening in, and measuring the incidence and nature of adverse drug events suffered by patients. The system is designed to alert physicians about critical detected events, and certain triggers will result in automated reports that will be evaluated on a daily basis by pharmacists trained in adverse drug event investigation.

The North Carolina Emergency Department Database (NCEDD) project, begun in 1999, created an emergency department data repository for the North Carolina Division of Public Health. NCEDD collected, standardized, and analyzed timely and secure emergency department data. The NCEDD led to the 2005 launch of the North Carolina Hospital Emergency Surveillance System (NCHESS), a mandated emergency department collection system that is expected to assist the State in early detection of and response to public health emergencies or potential biological or chemical terrorist attacks. A related venture is the North Carolina Disease Event Tracking and Epidemiologic Collection Tool (NC DETECT), an early event detection system allowing authorized users to view data from NCEDD and the Carolinas Poison Center, NC Wildlife Center, and other data sources for a variety of public health surveillance needs.

The University of North Carolina Hospital System is implementing a Perinatal EMR project, involving an electronic version of prenatal medical records integrated into software that will facilitate the input, storage, retrieval, and modification of prenatal medical records. The software also will allow patient access to medical data through a wireless LAN. The data will be transferred to and from a centralized database and can be shared with others over the Internet for clinical and research purposes. Another initiative focusing on children's health care is the Provider Access to Immunization Registry Securely Project (PAiRS) system. Begun in 1998, PAiRS was an early, critical component in North Carolina's development of a statewide immunization registry, which was implemented in 2005.

In the private sector, various health care stakeholders are discussing and taking action to create and participate in regional health information organizations (RHIOs). The Western North Carolina Health Network, Inc., a consortium of 16 hospitals in the Blue Ridge mountains, is one of the first RHIOs in North Carolina. All of the hospitals are schedule to be connected by early 2007. The participants currently can view patient data from each of the other participating hospitals through a virtual electronic medical records system, and each authorized user has a standardized view of the data. The second phase of the project contemplates including clinician offices and clinics within the network for additional efficiencies.

Purpose of the HISPC Project

The purposes of the HISPC project are to address variations in organization-level business policies and state laws that affect privacy and security practices which, in turn, may pose challenges to interoperable health information exchange; to recommend solutions and implementation plans to reduce or eliminate those challenges; and to increase the level of expertise in and compliance with privacy protections within the health care community.

NC HISPC's goals are to:

1. identify current health care practices and challenges regarding the release and exchange of health information,
2. develop consensus-based solutions for interoperable electronic health information exchange (HIE) that protect the privacy and security of health information, and
3. recommend high-level plans to implement recommended solutions.

The North Carolina Health Information Privacy and Security Collaboration project recommends policy, technological, and legal solutions to the barriers or obstacles identified in the Assessment of Variations Report. In addition to identifying solutions, the Report also documents, for each potential solution, the HIE context, privacy and security domains affected, involved stakeholders, HIE barriers that are addressed, and each solution's stage of development.

Purpose of the Report

The purpose of Final Assessment of Variation and Analysis of Solutions Report is to document the policy, technological, and legal barriers or obstacles identified during the first phase of the Project. This report also will document each of the identified potential solutions, their HIE context, the privacy and security domains affected, the stakeholders involved, and the HIE

barriers being addressed by the proposed solutions.

Scope of the Report
This report integrates the interim versions of the Assessment of Variations and Analysis of Solutions reports previously submitted by North Carolina. The report contains the final analysis of policy, technological, and legal barriers to exchanging health information within North Carolina and its bordering states, and it describes in greater detail the proposed solutions intended to reduce or eliminate those barriers.

Limitations of the Report
The NC HISPC overcame several obstacles in order to collect the stakeholders' business practices, analyze the information, and create the deliverables. Some of the obstacles overcome included:

- Strict time limitations minimized ability to perform in-depth research of the legal barriers to information exchange

Limited financial resources were available to the project contributors

- Difficult to recruit stakeholders to participate in the project
- Stakeholders were hesitant to share their proprietary organizational practices
- Some of the scenarios did not relate to actual practice
- Project lacks authority to implement proposed solutions

NC HISPC Workgroup Composition

Project Governance
As the contractor to AHRQ, RTI International provided oversight by assigning a state liaison from RTI International and the National Governors Association to the NC HISPC. RTI's liaison identified and mitigated project risks, established centralized processes, and guided the NC HISPC toward timely submissions of project deliverables. The NGA liaison provided strategic insight and advice on the intersection between HISPC and related projects currently underway through other state and federal initiatives.

Project Management Office (PMO)
The PMO consisted of Holt Anderson, NCHICA Executive Director, as Project Executive; Angie Santiago, Sr. Systems Consultant for TM Floyd & Company, as the Project Manager; and Diana Gildea as the Project Coordinator. The PMO provided policy standards, templates, training, and project tools designed to establish a collaborative framework and positive work experience for the project's participants.

The NC HISPC PMO provided each co-chair with a NC HISPC Project Workbook that contained:

- Workshop training materials
- Project documents
- Contact information
- Policies & procedures
- Confidentiality agreement
- Time tracking
- Milestone report
- Project plan
- Miscellaneous Resources

Project Co-Chairs
The VWG was co-chaired by Jim Murphy from the NC Department of Health and Human Services Office of Medicaid Management Information Systems (NC DHHS MMIS), Mike Voltero, General Counsel to Blue Cross Blue Shield of North Carolina, and Roy H. Wyman, Jr., a partner at Williams Mullen Maupin Taylor. The SWG and IPWG were chaired by Dave Kirby, President of Kirby Information Management Consulting. The LWG was chaired by Patricia A. Markus, a partner at Smith Moore LLP.

NC HISPC Workgroups

The Variations, Legal, Solutions, and Implementation Workgroups are comprised of attorneys; practice managers; researchers; clinicians; and professionals in public health policy, health information management, and information security specializing in health information privacy and security who represent health care stakeholders such as consumers, health plans, professional organizations, health care facilities, laboratories, health care software vendors, and public health agencies.

The Variations Workgroup (VWG) conducted individual and group assessments to document the stakeholders' current practices if they were presented with each of the 18 health care scenarios provided by RTI. The VWG was charged with collecting the business practice data and identifying potential barriers to exchanging health information. The VWG was co-chaired by Jim Murphy from the NC Department of Health and Human Services Office of Medicaid Management Information Systems (NC DHHS MMIS), Mike Voltero, General Counsel to Blue Cross Blue Shield of North Carolina, and Roy H. Wyman, Jr., a partner at Williams Mullen Maupin Taylor.

The Solutions and Implementation Plan Workgroups (SWG and IPWG) reviewed the data collected from the VWG and developed solutions and implementation plans to reduce or remove the identified barriers. The SWG and IPWG were chaired by Dave Kirby, President of Kirby Information Management Consulting. The SWG and IPWG were comprised of members representing the following health care stakeholders: Blue Cross Blue Shield of North Carolina, Duke University Health System, eHealth Initiative, E-Tech Security Pro, NC DHHS Office of Medicaid Management Information Services, NC Department of Mental Health and Substance Abuse, Novant Health, and Radarfind.

The Legal Workgroup (LWG) analyzed the business practices provided by the VWG and identified legal sources of the barriers to exchanging health information. The LWG was chaired by Patricia A. Markus, a partner at Smith Moore LLP. The LWG was comprised of members representing the following health care stakeholders: Blue Cross Blue Shield of North Carolina, CareSpark, FirstHealth of the Carolinas, LabCorp, Williams Mullen Maupin Taylor, NC DHHS Department of Medical Assistance, NC Hospital Association, NC Medical Society, Pitt County Memorial Hospital, NC Health Information Management Association, Quintiles Transnational, MISYS, NC Office of Information Technology Services, and UNC Hospitals.

With the exception of the PMO, all project participants have voluntarily contributed their time and expertise to this project.

Final Assessment of Variation Report

Final Assessment of Variation Report

Assessment of Variation Methodology

RTI International provided NC HISPC with 18 scenarios to analyze along nine domains of privacy and security. Each scenario represented a business practice or health care scenario that required the exchange of health information between different entities within North Carolina and other states. The facilitators encouraged the interviewees to adopt assumptions relevant to the exchange of health information between them and other entities. Assumptions included the establishment of a provider – patient relationship, whether the exchange occurred via electronic transmission (EMR, email) or manual processes (phone). NC HISPC grouped the 18 scenarios into four sub-group work clusters based on the type of stakeholders interviewed, the legal sources for the barriers, the security domains relevant to the scenarios, and the field of expertise of each professional participant. The scenarios' four sub-group work clusters are:

NC HISPC Scenario Sub-Group Work Clusters

Sub-group 1: Patient Care Scenarios
1. Patient Care A (Emergency Transfer)
2. Patient Care B (Substance Abuse)
3. Patient Care C (Access Security)
4. Patient Care D (HIV and Genetics)

Sub-group 2: Payer Scenarios
5. Payment (EHR Access)
9. Pharmacy Benefit A (Mail Order)
10. Pharmacy Benefit B (Claims Savings)

Sub-group 3: Secondary Use Scenarios
6. RHIO (Data Access)
7. Research (Data Usage)
8. Law Enforcement (Test Results)
11. Operations and Marketing A (Rehab Center)
12. Operations and Marketing B (Birthing PHI)
14. Employment Information (Return to Work

Sub-group 4: Government, Public Health & Safety Scenarios
13. Bioterrorism Event (Anthrax Spread)
15. Public Health A (Active TB Carrier)
16. Public Health B (Newborn Screening)
17. Public Health C (Homeless Shelters)
18. Health Oversight (Legal Compliance)

The PMO developed a facilitator training program that included confidentiality reassurance, guidance to maintain objectivity, suggestions for how to focus discussions on the presented scenarios and work session questions, and re-capping information for the recorders. Rehearsals and mock sessions were included in each training workshop.

Each VWG session was facilitated and recorded by one or more of the project Co-Chairs, the Project Manager, and the Project Coordinator.

In preparation for assessment sessions, the Co-Chairs reviewed data gathering requirements within the assessment tool, the statement of work in the proposal, and formulated a set of questions to focus on the "who, what, how, and why" of the organization's business practices around sharing information that correlated to the assessment tool fields. These are the questions each interviewee was asked:

1. What is your stakeholder type?
2. What is your current business practice if presented with this type of scenario?
3. Why is that your current business practice?
4. Does this business practice aid the exchange of health information with other entities?
5. Does this business practice present a barrier to exchanging health information?
6. Is this barrier appropriate to safeguard the information?
    a. Why is it appropriate?
    b. If not, could you recommend an alternate solution to removing this barrier?
7. How is this particular business practice affected in a manual or electronic environment?

These seven questions guided the Workgroups as they documented the practices shared by the stakeholders, identified barriers and their legal sources, and developed solutions and implementation plans to reduce or eliminate the barriers to exchanging electronic health information.

At each VWG session, the host welcomed the participants, introduced the facilitators and recorders, and then read the Rules of Engagement:

1. There are no right or wrong answers here. You are the expert!
2. Respond but don't consult or debate.
3. Respect the need for time for others to contribute. Be brief**.**
4. Everything shared or gathered is confidential.

In total, NCHICA hosted six group interviews, attended by 52 interviewees. Because of the low number of business practices collected, the PMO directly contacted certain stakeholders to inquire about their lack of response. Of the 20 stakeholders contacted, 9 intended to participate but were unable to leave work to attend a VWG session.

The remaining 11 stakeholders were prohibited by their organizations from sharing their proprietary practices. The organizations' reasons for not participating in the Assessment of Variation process were:

1. Unfamiliar with RTI International sufficient to trust in the confidentiality of the process.
2. Liability concerns regarding non-compliance or incorrect standards of practice.
3. Ambiguity of open-ended question format , as opposed to responding to specific surveys.

To mitigate the risk of distrust, the Steering Committee advised the Project Team to schedule onsite interviews. These were facilitated by the Project Manager and recorded by the hosting organization. Onsite interviews occurred at four area hospitals, two self-insured companies with a workforce size of 300-400 employees, and three group physician practices. Assessments were conducted in group and individual formats, depending on the comfort level of the interviewees. The onsite interviews proved successful and resulted in the collection of a full set of business practices for Groups 1, 3, and 4. Group 2 (Pharmacy Benefit Management) continues to show a deficit in the amount of stakeholder response.

The following steps were taken to identify the legal drivers to the information-sharing business practices:

1. The LWG reviewed the scenarios.
2. The LWG researched the NC and federal laws relevant to the type of health information exchange addressed in each scenario.
3. Then the LWG was given access to the results of the assessment sessions. The group reviewed the interviewees' current practices and policies.
4. The LWG identified the gaps between the relevant laws and the current understanding and application of those laws by the various health organizations.
5. The LWG recommended solutions to the legal barriers presented. The group also advised the SWG on proposed policy solutions which either may pose a liability risk to stakeholders or may conflict with state or federal law.

The HISPC Domains of Privacy and Security

RTI supplied the NC HISPC team with a set of domains to consider as the SWG and LWG considered solutions. This set of domains is derived from standard information security principles. Domains 1 - 6 are relevant to organizations that have implemented electronic health information systems. Due to the limited amount of implemented technology among the interviewees, most of the barriers that were identified centered around domains 7 – 9.

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

Stakeholder Responses

The following chart depicts the numbers and types of stakeholders who responded to the assessment of scenarios.

Scenarios	1. Clinicians	2. Physician groups	3. Federal health facilities	4. Hospitals	5. Payers	6. Public Health agencies	7. Community clinics and health centers	8. Laboratories	9. Pharmacies	10. Long term care facilities and nursing homes	11. Homecare and Hospice	12. Law Enforcement/ Correctional facilities	13. Professional associations and socieities	14. Medical and Public health schools	15. Quality improvement organizations	16. Consumers	17. State govt.	18. Other, specify
1. Patient Care - Scenario A (Emergent Transfer)	2	2	0	3	5	4	0	3	1	0	0	0	3	2	0	0	2	2
2. Patient Care - Scenario B (Sub Abuse)	2	2	0	3	5	4	0	3	1	0	0	0	3	2	0	0	2	2
3. Patient Care - Scenario C (Access Security)	2	2	0	3	5	4	0	3	1	0	0	0	3	2	0	0	2	2
4. Patient Care - Scenario D (HIV and Genetic)	2	0	0	3	5	4	0	3	1	0	0	0	3	2	0	0	2	0
5. Payment Scenario	1	0	0	5	6	0	0	0	0	0	0	0	0	0	0	0	0	0
6. RHIO Scenario	2	0	0	3	5	4	0	3	1	0	0	0	3	2	0	0	2	2
7. Research Final Scenario	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8. Law Enforcement Final Scenario	2	0	0	3	5	4	0	3	1	0	0	5	2	2	0	0	2	2
9. Pharmacy Benefit Final Scenario A	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0
10. Pharmacy Benefit Final Scenario B	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11. Operations and Marketing Final Scenario A	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	2
12. Operations and Marketing Final Scenario B	1	0	0	2	2	0	1	0	0	0	0	0	0	0	0	0	0	2
13. Bioterrorism Event Final Scenario	1	0	0	3	0	2	0	0	0	0	0	5	2	1	0	0	2	0
14. Employment Information Final Scenario	2	2	0	3	4	0	0	2	0	0	0	0	2	0	0	8	3	0
15. Public Health Final Scenario A	2	2	0	3	0	2	1	1	0	0	0	0	0	0	0	0	0	0
16. Public Health Final Scenario B	1	2	0	2	0	0	1	0	0	0	0	0	1	0	0	2	2	0
17. Public Health Final Scenario C	2	2	0	2	0	0	0	0	0	0	0	0	2	3	0	2	0	0
18. Health Oversight Final Scenario	1	0	0	2	2	2	0	0	0	0	0	0	0	0	0	0	0	3

Summary of Relevant Findings

Sub-Group 1: Patient Care Direct Treatment Scenarios

1. Patient Care A (Emergency Transfer)
2. Patient Care B (Substance Abuse)
3. Patient Care C (Access Security)
4. Patient Care D (HIV and Genetics)

Sub-Group 1 Stakeholders

Twenty-nine respondents participated in the assessment sessions for Sub-Group 1, the patient care scenarios. They included physician groups, clinicians, hospital health information managers (HIM) and nursing staff, researchers, hospital privacy officials, and health law attorneys (who responded on behalf of their hospital clients or were familiar with hospital operational issues).

The stakeholders reviewed the scenarios and described their organizations' practices with regard to each scenario.

An overview of the barriers identified by the VWG and LWG is below:

Stakeholders' Responses - Barriers Sub-Group 1: Patient Care Scenarios				
Barriers	SC - 1	SC – 2	SC – 3	SC - 4
BR_1. Misinterpretation of laws		29		
BR_2. Lack of business incentives				
BR_3. Lack of policy				
BR_4. Lack of security		29		
BR_5. Lack of interoperability	29			
BR_6. Lack of technology	29			
BR_7. Conflicting laws		29	29	29

Privacy and Security Domains Addressed

Domains Represented Sub-Group 1: Patient Care				
Domains	Scenario 1	Scenario 2	Scenario 3	Scenario 4
1. Authentication	X		X	
2. Authorization	X	X	X	X
3. Identity Matching	X	X	X	X
4. Transmission	X	X	X	X
5. Integrity			X	
6. Event Audit			X	X
7. Safeguards			X	
8. Data classification	X			X
9. Policies	X	X	X	X

Scenario 1: Patient Care A (Emergency Transfer)

Patient X presents to emergency room of General Hospital in State A. She has been in a serious car accident. The patient is an 89-year-old widow who appears very confused. Law enforcement personnel in the emergency room investigating the accident indicate that the patient was driving. There are questions concerning her possible impairment due to medications. Her adult daughter informed the ER staff that her mother has recently undergone treatment at a hospital in a neighboring state and has a prescription for an antipsychotic drug. The emergency room physician determines there is a need to obtain information about Patient X's prior diagnosis and treatment during the previous inpatient stay.

Scenario 1 Stakeholder Response

All clinical respondents agreed that the physician must first determine whether the patient is competent to make, or capable of making, decisions regarding her healthcare. This also determines the patient's ability to give consent for treatment or to release her health information.

Some physician stakeholders reported that typically the treating physician would verify the daughter's identity to confirm that she may authorize the treating hospital to obtain health information about her mother and to treat the patient. As the clinicians evaluate the patient's physical situation, they simultaneously determine the patient's state of mental health, gather her health history by obtaining the contact information of her primary and mental health care providers, and begin tracking the patient's prescription history.

Because the patient is from another state and would not have any medical records in the hospital at which she has presented, the requesting hospital's ER staff would contact the out-of-state hospital and the other providers who have previously treated the patient. Unless both hospitals and all providers involved in the patient's care are from the same health care system, it is likely that their health information systems would not be capable of sharing health information without customized software programs. Even if the hospitals had the same software, it is not common practice for a health care entity to give pre-authorized access to a patient's health information to persons or entities who do not have a treatment relationship with their patients; therefore, the requesting hospital's ER staff likely would not be able to access electronically the patient's health records.

All communications and requests for information would begin with the requesting hospital placing a phone call to the out-of-state hospital and faxing written authorization from the daughter to release the patient's health care information. Although all respondents agreed that it is not necessary to obtain authorization to request information from a patient or her legal representative during an emergency situation, they nonetheless would obtain and send an authorization to the sending hospital to "ease" the potential concerns of the sending hospital's staff regarding release of such information.

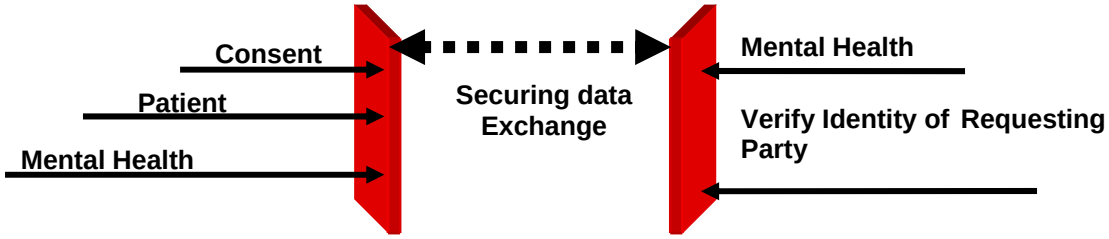
Because HIPAA requires that covered entities verify the identity and authority of persons requesting protected health information (§ 164.514 (h)(1)), the sending hospital would verify that the requestor is on duty at the ER by calling the main number of the hospital and transferring into the ER. If the sending hospital employs a full electronic health record, providing the requested information on the patient would be as simple as making an electronic chart request, printing the requested information, and faxing it to the requesting hospital.

If the sending hospital employs a mixed paper and electronic patient record platform, the patient's health information may be stored in more than one location within the hospital. In this case, the medical records department may act as a collection conduit and gather the requested information from the various storage locations. Depending on the time between the patient's treatment in the sending hospital and the current incident, the information at the sending hospital may not all have been dictated, and the hospital may not yet have final lab results or reports in the patient's record.

In order to obtain the additional information the requesting hospital needs to treat the patient, the sending hospital would obtain the patient's original written health information from the various departments in which the patient was treated. Although § 164.528(a) of HIPAA does not require an accounting of disclosures of information used for treatment purposes, it appears to be common practice for hospitals to make note of such copies and releases in the patient's chart, including the request for information by the requesting physician.

Finally, the sending hospital would ask the requesting hospital to send it the outcomes of the patient's treatment for follow up.

Scenario 1 Barriers



BR_5. Lack of interoperability between processes and technology: There is a potential for a delay in the exchange of health information between entities that practice in a paper or a mixed paper and electronic environment.

BR_5. Lack of interoperability between processes and technology: Depending on the time between the patient's treatment in the sending hospital and this incident, the information at the sending hospital may not all have been dictated, and the hospital may not yet have final lab results or reports in the patient's record.

Scenario 2: Patient Care B (Substance Abuse)

> An inpatient specialty substance abuse treatment facility intends to refer client X to a primary care facility for a suspected medical problem. The two organizations do not have a previous relationship. The client has a long history of using various drugs and alcohol that is relevant for medical diagnosis. The primary care provider has requested that the substance abuse information be sent by the treatment facility. The primary care provider intends to refer the patient to a specialist and plans to send all of the patient's medical information, including the substance abuse information that was received from the substance abuse treatment facility, to the specialist.

Scenario 2 Stakeholder Response
The clinical respondents indicated that it is not unusual for persons who are undergoing substance abuse treatment to also have need for medical care. Facilities will have contact with certain providers and have certain requirements to qualify for such programs. Upon admission, the individual or their representative would complete the appropriate forms that permit the facility to treat the individual and bill either the individual, a health plan, or special program.

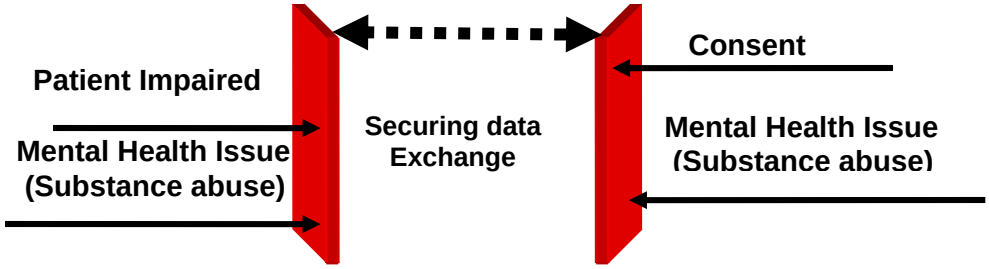
Prior to the patient's arrival, the primary care physician (PCP) may request the information from the facility. The facility is required to obtain an additional authorization from the individual in order to release the information to the provider. When the individual arrives at the primary care physician (PCP) for care, the individual will complete several forms including demographics and contact information, medical history, and an additional authorization for the PCP to send the information back to the treatment facility. The PCP will conduct an evaluation, diagnosis, and treatment plan. In this scenario the individual will sign three authorizations.

The clinicians are not sure why so many authorizations are required if the treatment facility referred the individual to them in the first place. The assumption is that HIPAA and North Carolina law requires the additional authorizations. All clinicians were aware that the individual has the right to restrict his or her information, even to the treating PCP, which raises concerns of whether or not the clinician has all of the information to render a proper diagnosis. If the clinician is unsure if the individual is providing sufficient information, he or she may be inclined to order additional lab tests. In the event that the individual is

diagnosed with a communicable disease, the physician is required to report that information to the local County Health Department.

The information exchange in this scenario is strictly by way of paper and faxing.

Scenario 2 Barriers:



BR_1. Range within organizations of misinterpretation and/or application of laws or regulation: VWG stakeholders responding to the survey stated that they would not release mental health information without patient consent because they were not aware that NCGS §§ 122C-55(d) and (e) allow it. The stakeholders' broad range of awareness and interpretation of North Carolina statutes may be symptomatic of a lack of judicial or administrative application or interpretation of such laws. Alternatively, it may be due to the stakeholders' lack of awareness of the manner in which such laws have been construed and applied, and the general lack of education about these laws.

BR_7. Conflicting or outdated federal or state laws or regulations: NCGS § 122C-55(i) allows for release of mental health and substance abuse information to the physician or psychologist who referred a patient to the facility, but it fails to provide for release of this information to any other physician (such as a primary care provider or specialist).

> Recommendation: Consider revising NCGS § 122C-55(i) to permit disclosure of this information to all providers treating the patient, recognizing that the effectiveness of the amendment may depend upon revision to the federal regulations regarding substance abuse treatment information, addressed below (42 CFR §§ 2.1 and 2.2).

BR_7. Conflicting or outdated federal or state laws or regulations: 42 CFR §§ 2.1 and 2.2: For release or re-release of substance abuse treatment information to third parties, federal law requires patient authorization or a court order, and it further requires the releasing party to provide notice of these restrictions upon any re-disclosure of such information (42 CFR § 2.32).

BR_7. Conflicting or outdated federal or state laws or regulations: Due to the requirements within 42 CFR §§ 2.1 and 2.2 for additional authorization from the patient to re-disclose substance abuse treatment information, the clinical stakeholders and the LWG are concerned that the treating physician may treat the patient with incomplete information.

BR_4. Lack of security standardization across entities; BR_5. Lack of interoperability between processes and technology: For facilities that receive federal funding, 42 CFR §§ 2.1 and 2.2 pre-empt NCGS § 122C-55(i). Substance abuse information is specially protected, so a consent for release must specify release of this information. Some hospitals include a space on their general consent forms for patients to initial in the event that the patient agrees to allow the hospital to release health information regarding the patient's substance abuse. Because substance abuse information is specially protected, it also needs to be segregated in the medical record in order to maintain such special protection, whether

the record is maintained in paper or electronic format. Some facilities have policies specifying that substance abuse information must be maintained separately in the patient's medical record.

Scenario 3: Patient Care C (Access Security)

At 5:30 pm Dr. X, a psychiatrist, arrives at the skilled nursing facility to evaluate his patient, recently discharged from the hospital psychiatric unit to the skilled nursing facility. The hospital and skilled nursing facility are separate entities and do not share electronic record systems. At the time of the patient's transfer, the discharge summary and other pertinent records and forms were electronically transmitted to the skilled nursing home.

When Dr. X enters the facility, he seeks assistance locating his patient, gaining entrance to the locked psychiatric unit, and accessing the patient's electronic health record to review the discharge summary, I&O, MAR and progress notes. Dr. X was able to enter the unit by showing a picture identification badge, but was not able to access the EHR. As it is Dr. X's first visit, he has no login or password to use their system.

Dr. X completes his visit and prepares to complete his documentation for the nursing home. Unable to access the skilled nursing facility EHR, Dr. X dictates his initial assessment via telephone to his outsourced, offshore transcription service. The assessment is transcribed and posted to a secure web portal.

The next morning, from his home computer, Dr. X checks his e-mail and receives notification that the assessment is available. Dr. X logs into his office web portal, reviews the assessment, and applies his electronic signature.

Later that day, Dr X's Office Manager downloads this assessment from the web portal, saves the document in the patient's record in his office and forwards the now encrypted document to the long-term care facility via e-mail.

The skilled nursing facility notifies Dr. X's office that they are unable to open the encrypted document because they do not have the encryption key.

Scenario 3 Stakeholder Response

All physician respondents stated that the skilled nursing facilities (SNF) in which they practice do not have an electronic health record environment. Therefore, reference to the electronic health record environment procedures in this scenario is hypothetical.

All respondents reported that a physician must first go through a rigorous credentialing process in order to obtain privileges to practice medicine in a facility and to access a particular unit. In order to obtain physical access to a unit, typically an authorization form is completed by Human Resources or Administration. This form may indicate the level of privileges the physician is granted within the facility. Some respondents stated that physicians may be required to obtain additional authorization to receive access to the behavioral health unit. According to the Information Technology (IT) departments represented, there are several reasons why the physician may have physical access to the unit but may not have access to the facility's information systems:

1. There may be a backlog of requests to gain access to the information system.
2. The physician may be required to attend orientation and computer training prior to obtaining access to the hospital's information system.

All respondents stated that they are aware of situations in which physicians have received access to their organization's computer systems regardless of whether formal authorization has been given. Upon showing the unit his or her credentials, the physician requests access to the patient's health information, and a staff member could log in to the system on behalf of the physician. When asked what their policy was on shared access, all respondents reported that shared access is against their organization's policy. When asked why they would risk breaking policy to allow the physician access to the electronic health

record, the staff members acknowledged that if the record was all paper, then the physician could obtain it easily from the cabinet and since the information was electronic, they did not see a reason not to share their access with the physician in order to enable the physician to treat the patient. Some respondents even stated that HIPAA allowed for the sharing of access to information as long as providing the access was for the purpose of treating a patient.

The physicians reported that they would prefer to have a print out of the patient's information rather than to obtain access to the information through the staff nurse. The physicians noted that their preference for the print out allows them to take the information with them to the patient's room to conduct their consult.

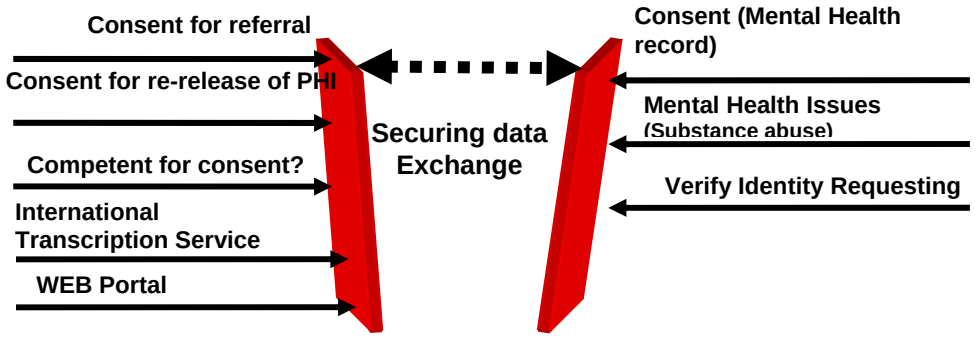
From a legal standpoint, in order to for the hospital to be able to release the patient's information to the SNF under NCGS § 8-53, the hospital's general consent form should provide that the patient consents to the release of his health information to third parties for purposes of treatment, payment, or health care operations. The SNF should include a similar provision in its general consent form in order for the physician to access the patient's information from the SNF.

All respondents stated that their organizations prohibit the outsourcing of transcription services to offshore companies. All respondents believed that the transcription company would be in violation of its contract if it outsourced its services to an offshore service without informing the physician and the SNF of this practice. One respondent noted that transcription companies, which are business associates to the physician and SNFs, would have to enter into a business associate agreement with the offshore service in order to provide the physician's or the SNF's patient information to the offshore company.

Current transcription is performed onsite and remotely by staff and contractors. Some physicians reported that they would dictate into the SNF's transcription system and would not need a business associate agreement with the transcription service because the contract is between the SNF and the transcription company. If the patient was seen in the physician's office, then the physician would dictate into his own transcription company. Other physicians responded that they would dictate into their own transcription service and send a signed copy of the notes to the SNF.

All respondents stated that they would not send a patient's assessment to the physician's personal e-mail account. The only way the physician would receive access to the patient's electronic information would be through the SNF's system.

Scenario 3 Barriers



BR_7. Conflicting or outdated federal or state laws or regulations: The barrier here is that there is no easy access to the patient's PHI at the SNF unless the patient has signed a general consent at the hospital that includes consent for release of information for treatment, payment, or health care operations purposes (thereby complying with NCGS § 8-53).

BR_7. Conflicting or outdated federal or state laws or regulations: Confidentiality of DNA: NCGS §§ 58-3-215 & 95-28.1a. There is nothing in this state statute that clearly requires additional authorization for release of a person's DNA information. It is left to the releasing entity to develop safeguards for such a release. The LWG generally agreed that the patient should be asked to give additional "special" authorization to release this information.

BR_6. Lack of workable technology: It is difficult to unbundle sensitive information from the overall electronic record. Once such information is there, the systems are not designed to block out parts of the record which are not deemed to be part of the legal health record or designated record set. The SWG will consider whether audit logging would be a feasible solution for providers who choose to allow open access to the clinical systems for all direct patient care staff.

- SOL_2. Implement policy standards, such as model policy and legislation, to address the complexity and ambiguity surrounding the release of information.
- SOL_2a. Implement security standards to address the complexity and ambiguity surrounding the safeguarding of health information.

BR_4. Lack of security standardization across entities; BR_6. Lack of workable technology: Audit logging: If unbundling electronic health information within an electronic health record may not be feasible, is it a viable solution to consider allowing open viewing access to a patient's electronic record to ensure continuity of care? Is an internal audit policy supported by a robust application audit logging capability sufficient to monitor the activity of the users and deter inappropriate accessing of this sensitive information?

BR_4. Lack of security standardization across entities; BR_6. Lack of workable technology: Implementation Barrier: Role-based access: The VWG and LWG recognize that role-based access could solve the minimum necessary requirements within HIPAA, as well as reduce the threat of unauthorized access to health information. However, applying role-based access in the treatment continuum also could create barriers to exchanging health information. The SWG will continue to collaborate with the LWG to identify potential solutions and the implementation barriers of role-based access in the health care setting.

Scenario 4: Patient Care D (HIV and Genetics)

Patient X is HIV positive and is having a complete physical and an outpatient mammogram done in the Women's Imaging Center of General Hospital in State A. She had her last physical and mammogram in an outpatient clinic in a neighboring state. Her physician in State A is requesting a copy of her complete records and the radiologist at General Hospital would like to review the digital images of the mammogram performed at the outpatient clinic in State B for comparison purposes. She also is having a test for the BrCa gene and is requesting the genetic test results of her deceased aunt who had a history of breast cancer.

Assumptions:

- Imaging centers do not perform complete physicals, they perform mammograms only.
- Primary care physicians perform a physical examination, but do not provide genetic testing or counseling. They would refer such testing or counseling to a specialist.
- This scenario includes the non-emergent transfer of health information.
- The physician would have received the patient's records prior to the appointment.

Scenario 4 Stakeholder Response

The respondents from institutional labs reported that NC does not permit clinical laboratories to release lab test results directly to the patient. However, if the state in which the patient resides permits or requires

disclosure to the patient, then the reference lab will make the disclosure. The respondents from the independent labs stated that it is common practice for patients not to have direct access to their lab results from the clinical laboratory. Instead, patients can and do obtain their test results from the ordering physician.

Because normally the primary care physicians would refer patients to a specialist for genetic testing, they are aware of state laws requiring genetic counseling when such tests are ordered, thus justifying the need for a referral to a genetic specialist. The physician respondents also were unaware of how HIPAA applies to decedents. They were uncertain whether the Minimum Necessary rule applied to the disclosure of health information, and they also were uncertain whether the niece would need to obtain authorization from the aunt's estate or next of kin in order to receive such information.

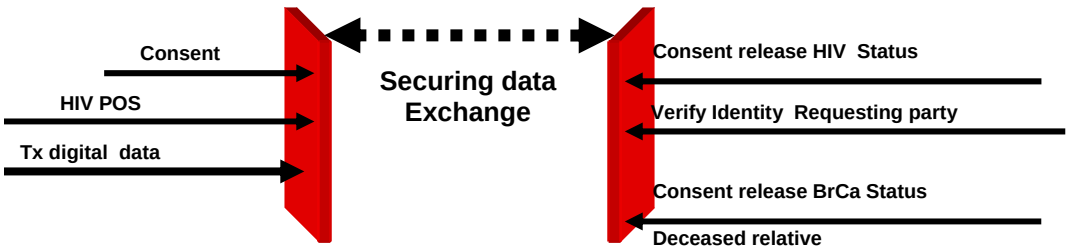
Other physicians argued that because the breast cancer gene is a gene that could have been passed down from the aunt, the niece should have access to the aunt's health information. According to this school of thought, if a provider thought it was pertinent, then the deceased relative's genetic information could be considered "treatment" information for the current patient, and thus an authorization to obtain the data would not be needed.

However, if the information regarding the aunt's breast cancer is not sufficiently related to the patient, then an authorization from the next of kin or the estate would be needed.

All physicians were aware of the NC law requiring counseling when a patient requests HIV testing. The NC statute that supports this practice is NCGS §130A-148.

Respondents from the medical records community stated that if such a request was presented in their department, they would release the information to the physician but possibly not directly to the patient. Some hospitals require specific patient consent before releasing genetic information.

Scenario 4 Barriers



BR_7. Conflicting or outdated federal or state laws or regulations: It is uncertain how the DNA information might be used in the future. HIPAA does not specifically address use and disclosure of this type of information. The LWG recognizes the sensitivity of genetic information and the manner in which this information could be used inappropriately, and it is concerned that the absence of limitations on the transfer of such information will serve as a barrier to exchanging this information, particularly with respect to patients who may simply refuse to advise their health care providers about this information. Nonetheless, the LWG is hesitant to recommend additional safeguards for maintaining the confidentiality of such information that may be construed broadly enough to pose barriers to future research and treatment.

Sub-Group 2: Payment Scenarios

5. Payment (EHR Access)
9. Pharmacy Benefit A (Mail Order)
10. Pharmacy Benefit B (Claims Savings)

Sub-Group 2 Stakeholders

Nine individuals responded to scenario 5. They included staff members from the payer community who specialize in case management, health, and corporate law. Respondents to scenario 7 included HIPAA privacy officials, physician group administrators, health information professionals, clinicians, and research professionals. No pharmacy benefit managers responded to the invitations to participate in the assessment regarding scenarios 9 and 10.

The stakeholders reviewed the scenarios and described their organizations' practices with regard to each scenario.
An overview of the barriers identified by the VWG and LWG is below:

Stakeholders' Responses - Barriers Sub-Group 2: Payer / PBM Scenarios			
Barriers	SC – 5	SC – 9	SC - 10
BR_1. Misinterpretation of laws			
BR_2. Lack of business incentives			
BR_3. Lack of policy			
BR_4. Lack of security			
BR_5. Lack of interoperability	9		
BR_6. Lack of technology	9		
BR_7. Conflicting laws			

Privacy and Security Domains Addressed

Domains Represented Sub-Group 2: Payer / PBM				
Domains	Scenario 5	Scenario 7	Scenario 9	Scenario 10
1. Authentication	X			
2. Authorization	X			X
3. Identity Matching	X		X	
4. Transmission	X		X	
5. Integrity		X		X
6. Event Audit	X	X		
7. Safeguards				
8. Data classification		X	X	
9. Policies	X	X	X	X

Scenario 5: Payment

X Health Payer (third party, disability insurance, employee assistance programs) provides health insurance coverage to many subscribers in the region the health care provider serves. As part of the insurance coverage, it is necessary for the health plan case managers to approve/authorize all inpatient encounters. This requires access to the patient health information (*e.g.*, emergency department records, clinic notes, etc.).

The health care provider has recently implemented an electronic health record (EHR) system. All patient information is now maintained in the EHR and is accessible to users who have been granted access through an approval process. Access to the EHR has been restricted to the health care provider's workforce members and medical staff members and their office staff.

X health Payer is requesting access to the EHR for their accredited case management staff to approve and authorize inpatient encounters.

Scenario 5 Stakeholder Response
Payer information is obtained from providers and facilities via paper and electronic batches. All payer information is considered "second–hand" information. It is assumed that the data has not been altered.

Payers require the patient's health information to assist in the coordination of referrals and to process claims. Claims are often denied for lack of information. Once more information is obtained from the physician or facility the claim can be reevaluated.

Payer case management respondents stated that they would never access a provider's EHR
Because case managers focus on coordinating the patient's care with providers, they typically request the patient's entire record to help identify the patient's problem, necessary or predicted length of stay, and whether third party vendors will be used to process the claims.

Physicians provide requested patient information in either paper or electronic format. When asked if the provider would ask for an authorization from the patient, the payer respondents indicated not usually, because payers also are covered entities. When asked if minimum necessary rules apply to disclosures to the payer, payer respondents indicated that while such rules may apply, often the physicians do not give the case managers enough information to determine pre-certification authorization, so the payer ends up requesting the entire patient chart.

Because payers have hundreds of plans and thousands of providers, their ability to access the individual health care providers' EHRs may not be feasible or necessary to conduct their business. Payers do receive batch information from the facilities and providers who participate in the Electronic Data Interchange (EDI) services.

Claim processing complexities include the type of facility and service involved, if the service must be pre-certified, and the type of contract. Some hospitals are supposed to send records to the payer daily. In order for the provider to be paid and accept assignment, the payer case managers will follow up with the provider to ensure that all of the patient's information required for pre-approval of payment is obtained. However, the responsibility for ensuring that all of the required information is sent to the health plan belongs to the insured patients. They must work with their provider and their health plan to ensure that they understand all of their financial responsibilities, including release of information requirements.

Scenario 5 Barriers

BR_5. Lack of interoperability between processes and technology; BR_6. Lack of workable technology

Technological barriers between payers and individual and small physician groups delay the exchange of health information for the purpose of processing claims, and these barriers continue to increase the administrative costs for the health care providers and payers alike.

Scenario 9: Pharmacy Benefit A (Mail Order)

The Pharmacy Benefit Manager (PBM) has a mail order pharmacy for a hospital which is self-insured and also has a closed formulary. The PBM receives a prescription from Patient X, an employee of the hospital, for the antipsychotic medication Geodon. The PBM's preferred alternatives for antipsychotics are Risperidone (Risperdal), Quetiapine (Seroquel), and Aripiprazole (Abilify). Since Geodon is not on the preferred alternatives list, the PBM sends a request to the prescribing physician to complete a prior authorization in order to fill and pay for the Geodon prescription. The PBM is in a different state than the provider's Outpatient Clinic.

Scenario 9 Stakeholder Response
None

Scenario 9 Barriers
None identified

Scenario 10: Pharmacy Benefit B (Claims Savings)

A Pharmacy Benefit Manager 1 (PBM1) has an agreement with Company A to review the companies' employees' prescription drug use and the associated costs of the drugs prescribed. The objective would be to see if the PBM1 could save the company money on its prescription drug benefit. Company A is self-insured and as part of its current benefits package, has the prescription drug claims submitted through its current PBM (PBM2). PBM1 has requested that Company A send its electronic claims to them to complete the review.

Scenario 10 Stakeholder Response
None

Scenario 10 Barriers
None identified

Sub-Group 3: Secondary Use Scenarios

Group 3 scenarios were based on the uses and disclosures of health information for the purposes of conducting health care operations, marketing, or work-related activities which have no impact on direct patient care.

6. RHIO (Data Access)
7. Research (Data Usage)
8. Law Enforcement (Test Results)
11. Operations and Marketing A (Rehab Center)
12. Operations and Marketing B (Birthing PHI)
14. Employment Information (Return to Work)

Sub-Group 3 Stakeholders

The 27 respondents for scenario 6 included individuals representing clinicians, hospitals, health plans, public health agencies, laboratories, pharmacies, professional associations, and academic medical centers. The 32 respondents for scenario 8 included individuals representing clinicians, hospitals, payers, public health agencies, laboratories, pharmacies, law enforcement, professional associations, academic medical centers, county government, and the legal community. The 5 respondents for scenarios 11 and 12 (Group 3 Health care Marketing and Operations) included marketing professionals that specialize in hospital wellness programs from the hospital, payer, and disease management communities. The 26 respondents for scenario 14 (Employee Health Information) included human resource professionals and employees from self-insured employers, payers, academic medical centers, hospitals, and group practice administrators.

The stakeholders reviewed the scenarios and described their organizations' practices with regard to each scenario.

An overview of the barriers identified by the VWG and LWG is below:

Stakeholders' Responses - Barriers Sub-Group 3: Secondary Use of Health Information Scenarios						
Proposed Solutions	SC - 6	SC – 7	SC – 8	SC – 11	SC – 12	SC - 14
BR_1. Misinterpretation of laws				5	5	26
BR_2. Lack of business incentives		1				
BR_3. Lack of policy	27					
BR_4. Lack of security	27					
BR_5. Lack of interoperability		1				
BR_6. Lack of technology		1				26
BR_7. Conflicting laws	27		32			26

Privacy and Security Domains Represented

Domains Represented Sub-Group 3: Secondary Use of Health Information Scenarios						
Domains	SC - 6	SC – 7	SC – 8	SC – 11	SC – 12	SC - 14
1. Authentication		X		X		
2. Authorization	X		X	X	X	X
3. Identity Matching	X	X			X	
4. Transmission	X	X		X	X	X
5. Integrity	X	X				X
6. Event Audit	X			X		X
7. Safeguards	X					X
8. Data classification		X	X	X	X	
9. Policies	X	X	X	X	X	X

Scenario 6: RHIO

The RHIO in your region wants to access patient identifiable data from all participating organizations (and their patients) to monitor the incidence and management of diabetic patients. The RHIO also intends to monitor participating providers to rank them for the provision of preventive services to their diabetic patients.

Assumptions:

- The "RHIO" has entered into a formal business associate agreement with the stakeholder participants in the RHIO. All of the stakeholders have implemented an electronic practice management system and electronic health record.

Scenario 6 Stakeholder Response:
All stakeholder respondents stated that before they would agree to enter into a RHIO or a similar health information exchange agreement they would seek legal counsel to help them to identify and understand the RHIO's purpose, to determine how the patient information would be safeguarded and de-identified, and to review appropriate protections and rights for each stakeholder and its patients if patient information was inappropriately disclosed.

The physician respondents unanimously confirmed they would seek patients' authorization to use their information in a RHIO setting.

All respondents believed that exchanging patient information when participating in a RHIO type of arrangement is permitted under HIPAA as use or disclosure for treatment, payment, or health care operations. Although this scenario focused on diabetes management, the physician respondents did not generally agree that the use of this information should be categorized as treatment. The physicians argued that although the use of this information would have the benefit of long-term treatment protocols, their patients would not directly or immediately benefit from their participation in such an information exchange.

All respondents agreed that the information accessed by the RHIO for the purpose of monitoring the management of diabetic patients should be de-identified. The physicians also were uncertain about what kind of information they would submit for this purpose. They believed that different physicians differ in their treatment approaches, and that this may require different information to be submitted.

When asked what concerns they would have, the physicians, HIM, laboratories, payers, and software vendors all replied that they were concerned that the RHIO would want information that would not be related to effective treatment for diabetes. They were uncertain what recourse they would have if the RHIO used the information it accessed for another purpose or if the information was inappropriately used or released.

The software vendor stated that it removes fields from data to comply with HIPAA, and that it also hires a statistician to ensure that there is no way to re-link the identifiable information to individuals. The vendor reported that consent for use of data is generally a contractual obligation. An actuarial analysis of results by physician was recommended in order to determine which physician has best outcomes for the cost.

The laboratory respondents reported that in order for them to participate in the RHIO or a similar health information health exchange organization, they would be required to sign a HIPAA Business Associate Agreement with each participating health care stakeholder. Otherwise, the RHIO would have to obtain the lab test results directly from the test-ordering provider's system. However, since most physicians are still operating in a paper environment, they would not have the ability to send the lab information to the RHIO. The inability to send the lab test results directly to the RHIO could degrade the integrity of the information.

While the laboratory respondents stated that there was no NC statute that prohibits them from sending lab test results directly to the patient and that sending this information to patients is a matter of common practice in other states, they did offer CLIA (42 CFR § 493.1291(f)) as the legal barrier to their direct participation in a RHIO.

A respondent representing the retail pharmacy industry stated that adding retail pharmacies to a RHIO's membership may help with the management of chronic diseases. It is unknown whether there currently is a place for participation by retail pharmacy industry in RHIOs. Further research by the SWG is recommended. The pharmacy respondent stated that the Pharmacy Benefit Management community transmits and stores all of the prescription information for all of the pharmacy claims. This community may be a source of information for the RHIO.

It was confirmed that NC Division of Medical Assistance (Medicaid) acts as the State's Pharmacy Benefit Manager (PBM). NC Medicaid does not participate in any RHIOs at this time.

Most physicians did not feel that there was an incentive for them to exchange information with other entities, and they were uncertain whether and how the RHIO would benefit their practices financially.

Scenario 6 Barriers

BR_3. Lack of policy standardization across entities: There is no uniform definition of what a RHIO is, nor is a RHIO recognized as a specific legal entity in NC. AHIC is considering future projects that would formalize the various potential structures of RHIOs. The clinicians and the LWG are concerned that ranking providers based upon their participation in the RHIO and their patient outcomes would make it appear as if those providers who do not participate in the RHIO engage in sub-standard practices, and this appearance could be misleading. The providers who participate in the information exchange could be ranked higher than a physician not be involved in the RHIO simply due to such participation.

> **Recommendation:** Develop formal definitions and standards for RHIOs that have participating stakeholders in multiple states. Consider the purposes of sharing information in order to establish RHIO standards, definitions, criteria, organizational structures, sources of payment, and general guidance in order to assist the health care industry in appropriately sharing the information.

BR_2. Lack of business incentives to exchange information; BR_7. Conflicting or outdated federal or state laws or regulations: The LWG has some concerns about the outcomes-based compensation. If a "report card" for each participating provider was published, it is possible that a consumer may believe that a non-participating provider who in fact has poor outcomes has higher scores than a participating provider who may score fairly low based upon his patient-mix. It is also possible that an increase in referrals to physicians based upon their patient outcome rankings conflicts with NCGS § 90-401, which prohibits the compensation of physicians for referrals.

BR_7. Conflicting or outdated federal or state laws or regulations: Lab administration is experiencing difficulty with this barrier. The RHIO is not an "authorized person," as that term is defined by CLIA. The lab currently can release test results to the ordering physician, but the physician would need to authorize the lab to release the information to the RHIO. Accordingly, without a change in CLIA, agreements and contracts specifying the need for such physician authorization must be planned and implemented during the initial design of the RHIO. Once the design and contracts are in place, tests for the management of selected diseases could be sent automatically to the RHIO via electronic batches.

The make-up of and stakeholder participants in RHIOs vary, depending upon the main purpose(s) of the RHIOs. In regards to exchanging lab information, current federal and state laws have not addressed the need to identify RHIOs as "authorized users" for purposes of receiving lab test results directly from clinical laboratories.

BR_7. Conflicting or outdated federal or state laws or regulations: CLIA, 42 CFR § 493.1291(f): Test results must be released only to ***authorized persons*** and, if applicable, the individual responsible for

using the test results and the laboratory that initially requested the test. RHIOS do not fall under this category.

BR_7. Conflicting or outdated federal or state laws or regulations: CLIA, 42 CFR § 493.2 **"**Authorized person**"** means an individual authorized under state law to order tests or receive test results, or both. RHIOS do not fit in this category.

Recommendation: Revise CLIA regulations at 42 CFR § 493.1291(f) and 42 CFR § 493.2 to expand the list of permissible recipients of lab test results to include Covered Entities and Business Associates.

Scenario 8: Law Enforcement

An injured nineteen (19) year old college student is brought to the ER following an automobile accident. It is standard to run blood alcohol and drug screens. The police officer investigating the accident arrives in the ER claiming that the patient may have caused the accident. The patient's parents arrive shortly afterward. The police officer requests a copy of the blood alcohol test results and the parents want to review the ER record and lab results to see if their child tested positive for drugs. These requests to print directly from the electronic health record are made to the ER staff.

Scenario 8 Stakeholder Response
All emergency room respondents stated that they would not share information regarding the patient's condition with the patient's parents unless the patient either was present (which implies consent) or had provided a written authorization to share such information.

In order for law enforcement officers to obtain the blood alcohol test results, they would need to present a subpoena before a hospital would release the information. The hospital would include a copy of the subpoena in the patient's chart and include such release in their Accounting of Disclosures form.

Law enforcement respondents stated that their priority would be to conduct the investigation at the scene of the accident. Requesting the information from the hospital would normally follow at a later time with their preliminary reports and subpoena. However, the law enforcement respondents did report that depending on the severity of the accident and the condition of the patient or other victims, it would need to obtain statements from the patient, and this usually occurs in the ER. The law officers stated that they have not run into a problem obtaining information immediately following an accident while at the ER, but they often have problems obtaining final copies of the treatment reports from the medical records department.

The hospital staff also reported that if running the blood alcohol level test is part of the patient's treatment and is agreed to under the general consent, then the test will be run but the results will not be released to either the police or the adult patient's parents without the patient's consent. However, if the patient is unconscious upon admission to the hospital and the parents must consent on the patient's behalf for treatment pursuant to NCGS §90-21.13, the hospital may have to release information to the parents in order to describe the risks of treatment.

Scenario 8 Barriers
BR_7. Conflicting or outdated federal or state laws or regulations: NCGS § 20-16.2, a new law that became effective December 1, 2006, provides that an unconscious person can be required to undergo a blood alcohol level test, and police can test a coherent person; the consequence of refusing the test is having one's drivers license revoked. This is deemed an appropriate barrier to information exchange. This new statute is specific to patient information that may be disclosed to law enforcement where the patient is involved in a vehicle crash.

Scenario 11: Operations and Marketing

As per the instructions from the final scenario guidelines that state: *"Note: This scenario could be modified to apply to any health care provider (physician group, home health care agency, etc.) wishing to market services to a targeted subset of patients." T*he assessment was modified to concentrate on general health care marketing practices.

ABC Health Care is an integrated health delivery system comprised of ten critical access hospitals and one large tertiary hospital, DEF Medical Center, which has served as the system's primary referral center. Recently, DEF Medical Center has expanded its rehab services and created a state-of-the-art, stand-alone rehab center. Six months into operation, ABC Health Care does not feel that the rehab center is being fully utilized and is questioning the lack of rehab referrals from the critical access hospitals.

ABC Health Care has requested that its critical access hospitals submit monthly reports to the system six-sigma team to analyze patient encounters and trends for the following rehab diagnoses/ procedures:

- Cerebrovascular Accident (CVA)
- Hip Fracture
- Total Joint Replacement

Additionally, ABC Health Care is requesting that this same information, along with individual patient demographic information, be provided to the system Marketing Department. The Marketing Department plans to distribute to these individuals a brochure highlighting the new rehab center and the enhanced services available.

Scenario 12: Healthcare Operations and Marketing - Scenario B

ABC hospital has approximately 3,600 births/year. The hospital Marketing Department is requesting PHI on all deliveries including mother's demographic information and birth outcome (to ensure that contact is made only with those deliveries that resulted in healthy live births). The Marketing Department has explained that they will use the PHI for the following purposes:

- To provide information on the hospital's new pediatric wing/services.
- To solicit registration for the hospital's parenting classes.
- To request donations for construction of the proposed neonatal intensive care unit.

They will sell the data to a local diaper company.

Scenarios 11 and 12 Stakeholder Response

One hospital marketing representative responded that her group would consider programs that use de-identified patient information which allows them to identify trends in patient-mix, diseases, and treatment types. She reported that there were some special programs for new mothers with a direct marketing campaign. However, the mothers sign an authorization to receive such information at their doctor's office or at the hospital. She was unaware of and direct marketing for any other patient mix within her organization.

She did know that HIPAA was strict on marketing and assumed that was why she didn't have access to the patient's information.

When asked if the hospital had a foundation to help raise funds for various activities, she replied in the affirmative and is certain that they obtain direct patient information. When asked if patients were aware of

this activity when they register or are admitted, she stated that the information was on the consent form, but not in the Notice of Privacy Practices.

The remainder of the marketing representatives had heard of HIPAA but weren't sure why it would apply to their department. They stated that they did not receive training from their employers since HIPAA only applied to the clinical staff.

Scenarios 11 and 12 Barriers
BR_1. Range within organizations of misinterpretation and/or application of laws or regulation; BR_2. Lack of business incentives to exchange information; BR_3. Lack of policy standardization across entities: Marketing staff who participated in the assessment sessions stated that they are not required to participate in the hospital's HIPAA training. They state that since they don't deal with patient information, such training is not necessary; however, the LWG, health information security and IT staff believe that as health information exchanges result in more complicated contractual agreements and technological solutions, having a privacy and security expert act as a "consultant" to the marketing staff during proposed marketing strategies would be beneficial to the organization.

Scenario 14: Employee Work Note

An employee (of any company) presents in the local emergency department for treatment of a chronic condition that has exacerbated which is not work-related. The employee's condition necessitates a four-day leave from work for illness. The employer requires a "return to work" document for any illness requiring more than two days leave. The hospital ED has an EHR and its practice is to cut and paste patient information directly from the EHR and transmit the information electronically to the HR department.

Scenario 14 Stakeholder Response
Two employees in human resources stated that if the employee was sick or injured in a non work-related situation, the employee would submit a paper note to the Human Resources department upon his return to work. When asked if receiving the work note directly from the ER would help in their administrative duties, they stated that receiving the work note from the employee was sufficient.

Although they may call the emergency department to check on the condition of their employee, these HR employees stated unanimously that they would never engage an emergency department to obtain an employee's return to work note unless it was a Workers Compensation claim.

Scenario 14 Barriers

BR_5. Lack of interoperability between processes and technology; BR_6. Lack of workable technology: Unless the employee's absence was due to a work-related injury or illness, the employer is prohibited from requesting health information from the emergency room. In this particular scenario, only the employee has the authority to allow access to his or her health information. If the employer implemented a personal health record system like Dell, IBM, and Wal-Mart are offering to their employees, then the employee could voluntarily choose to send the information directly to the employer.

Sub-Group 4: Government, Public Health & Safety Scenarios

13. Bioterrorism Event (Anthrax Spread)
15. Public Health A (Active TB Carrier)
16. Public Health B (Newborn Screening)
17. Public Health C (Homeless Shelters)
18. Health Oversight (Legal Compliance)

Sub-Group 4 Stakeholders

Respondents to scenarios 13 and 15-18 (Group 4 Public Health and State Government) included NC state government employees representing public health agencies, substance abuse, mental health, emergency management, laboratories, hospitals, clinicians, medical and public health schools, health information management, disaster and homeland security professionals. There were no participants from drug treatment centers or homeless shelters.

The stakeholders reviewed the scenarios and described their organizations' practices with regard to each scenario. An overview of the barriers identified by the VWG and LWG is below:

Stakeholders' Responses - Barriers Sub-Group 4: State Govt. & Public Health Scenarios					
Proposed Solutions	SC – 13	SC – 15	SC – 16	SC – 17	SC – 18
BR_1. Misinterpretation of laws					
BR_2. Lack of business incentives					
BR_3. Lack of policy	19				
BR_4. Lack of security					
BR_5. Lack of interoperability	19	11			8
BR_6. Lack of technology		11			8
BR_7. Conflicting laws					
SOL_7. Amend laws			12	14	
SOL_8. Develop consumer programs					

Privacy and Security Domains Addressed

Domains Represented Sub-Group 4: State Govt. & Public Health					
Domains	Scenario 13	Scenario 15	Scenario 16	Scenario 17	Scenario 18
1. Authentication			X		X
2. Authorization	X	X	X	X	X
3. Identity Matching	X	X	X	X	X
4. Transmission		X	X	X	X
5. Integrity	X	X	X		X
6. Event Audit	X			X	X
7. Safeguards					X
8. Data classification	X	X	X	X	X
9. Policies	X	X	X	X	X

Scenario 13: Bioterrorism

A provider sees a person who has anthrax, as determined through lab tests. The lab submits a report on this case to the local public health department. The public health department in the adjacent county has been contacted and has confirmed that it is also seeing anthrax cases, and therefore it could be a possible bioterrorism event. Further investigation confirms that this is a bioterrorism event, and the state declares an emergency. This then shifts responsibility to a designated state authority to oversee and coordinate a response, and involves alerting law enforcement, hospitals, hazmat teams, and other partners, as well informing the regional media to alert the public to symptoms and seek treatment if they feel affected. The state also notifies the Feds (Homeland Security and CDC) of the event, and some federal agencies may have direct involvement in the event. All parties may need to be notified of specific identifiable demographic and medical details of each case as they arise to identify the source of the anthrax, locate and prosecute the parties responsible for distributing the anthrax, and protect the public from further infection.

Scenario 13 Stakeholder Response
Although NC has been exchanging epidemiological information for the purpose of tracking communicable diseases through the NC Public Health Information Network (NC PHIN), public policy regarding response to a possible bioterrorism event as presented in Scenario 13 posed a challenge for most of the respondents.

Government respondents (who did not include public health staff) stated that they would refer to the state's contact and initiative regarding bio-terrorism events in conjunction with the county health department. None of the respondents knew the responsibilities added to the role of county's or state's Health Director in the event of bioterrorism.

County health department administration noted that anthrax cases are to be reported to the county health department. While aware of the NC PHIN reporting system, the health department administrators were unaware that NC PHIN was implemented in North Carolina emergency departments only. Awareness programs regarding bioterrorism incident reporting were usually sponsored by the Department of Homeland Security, Emergency Management or Public Health. During the assessment, the county health departments had no specific plans to include private practice physicians in their bioterrorism community outreach program.

Law enforcement respondents, such as the sheriff or city police departments, stated they would assist in enforcement of a public health order upon its issuance from the county or state Health Director. Law enforcement and emergency management respondents clearly were aware of state policy as well as recent bioterrorism exercise drill outcomes or training; however, they were unaware of any statutes that prohibit access to health information to assist in the enforcement of a public health emergency.

Hospital staff stated that upon clinical diagnosis and confirmation from the laboratory results, they would implement the hospital's Hazmat protocol and report the incident to the county health department.

When asked what communicable diseases were reportable to the State, most physicians responded with less than half of the actual requirement. They were unaware that anthrax was a reportable communicable disease. Physicians in private practice were able to cite the procedures for diagnosis and treatment, but they were unsure to what individual or agency they should report an anthrax case; therefore, they would seek guidance from their local health department. Finally, the physicians stated that their practice management system does not report communicable diseases to the county or state. All communicable diseases are reported by phone.

Scenario 13 Barriers
BR_3. Lack of policy standardization across entities; BR_5. Lack of interoperability between processes and technology: NC receives epidemiological information from hospital or emergency

department information systems for the purpose of monitoring communicable diseases through the NC PHIN. However, group or individual physicians' practice management systems are not linked to this network. In order for a physician to report a communicable disease, he must contact the health department by phone and begin the manual process of copying or faxing the medical record to the department. For the group or individual physician, the time constraint between the diagnosis of a public health concern and the limited time available to complete the manual process of notifying the health department is an inappropriate barrier that impedes the exchange of electronic health information

Scenario 15: Public Health Active Carrier, Communicable Disease Notification

Active TB Patient has decided to move to a desert community that focuses on spiritual healing. The TB is classified MDR (multi-drug resistant). Patient purchases a bus ticket - the bus ride will take a total of nine hours with two rest stops. State A is made aware of Patient's intent two hours after the bus with Patient leaves. State now needs to contact the bus company and State B with the relevant information. State A may need to contact every state along the route.

Scenario 15 Stakeholder Response
The staff members interviewed from multiple state government agencies were mostly articulate in their agency's policy(ies) regarding the exchange of public health information within or across state lines as presented in scenario 15, where a TB active patient seeks treatment in another state. If the report was initiated from a health care or public health professional, the public health employees would notify their counterparts in the other states. However, due to their confidentiality policy and applicable laws, they stated they would be limited in their response if the report came from an individual.

Clinicians and physicians in private practice unanimously stated that if they were informed of a patient's intent to travel by public transport while undergoing TB treatment, they would report this incident to the county health department followed by faxing or mailing copies of the patient's medical record to the health department.

Scenario 15 Barriers
BR_5. Lack of interoperability between processes and technology; BR_6. Lack of workable technology: If the clinician followed NC law to report communicable diseases, the health department would have already had the patient's information. The reporting in this case was not that there was a case of TB but that the person was traveling to another state. As health information technology adoption increases, health departments will be able to exchange health information of this type in a timely fashion.

Scenario 16: Newborn Screening

A newborn's screening test comes up positive for a rare genetic disorder and the state lab test results are made available to the child's physicians and specialty care centers specializing in the disorder via an Interactive Voice Response system. The state lab also enters the information in its registry, and tracks the child over time through the child's physicians. The state public health department provides services for this rare genetic disorder and notifies the physician that the child is eligible for those programs. One of the services that the mother uses from the state is regularly purchasing special food products for persons with PKU.

Scenario 16 Stakeholder Response
The respondents from the public health, laboratory, clinician, and pediatric communities stated that under the authority of 10A NCAC § 43F.1203, the state of North Carolina will screen all newborns for permanent hearing loss. Due to the public health activity exclusion in HIPAA, there is no authorization required by the parent for a hospital to share the results of such screenings with the Early Intervention for Toddlers with Disabilities and Birth Defects and Women's Health Programs managed by the local health departments. In the event of a positive diagnosis, the state lab would notify the pediatrician, who would then notify the parents.

The local health department would determine program eligibility and contact the parents to facilitate parent education or a referral to a specialist for treatment. The health department respondents stated that the counties do not use a voice program to notify the parents of their results. The current practice is to call the parent and manually send a copy of the record to the treating specialist.

Overall, the VWG did not find any practice variances between the laboratory, pediatric, and county health department regarding NC's Newborn Screening Requirement practices. Concerns concentrated in the lack of electronic health information exchange between the interested stakeholders.

Scenario 16 Barriers
BR_7. Conflicting or outdated federal or state laws or regulations: All respondents agreed that NC's Early Intervention Programs do not pose a significant policy barrier. Overall, the VWG did not find any variances in practices or barriers in NC's Newborn Screening Requirement business practices. They perceived significant technological barriers that delay the exchange of health information between the stakeholders. While the State Lab and hospital information systems may interface with each other, pediatric or specialty practices which are not part of a particular organized health system may not have the ability to exchange electronic information with the hospital or lab without significant technological capital investments.

Scenario 17: Homeless Shelter

A homeless man arrives at a county shelter and is found to be a drug addict and in need of medical care. The person does have a primary provider, and is sent there for the medical care, and is referred to a hospital-affiliated drug treatment clinic for his addiction under a county program. The addiction center must report treatment information back to the county for program reimbursement, and back to the shelter to verify that the person is in treatment. Someone claiming to be a relation of the homeless man requests information from the homeless shelter on all the health services the man has received.

Scenario 17 Stakeholder Response
During the assessment, the respondents adopted the assumptions that the homeless individual was currently enrolled in a county-sponsored outpatient addiction treatment program which made him eligible to stay at the county shelter. For the purpose of simplifying the types of uses and disclosures of health information needed, the respondents assumed that the homeless man's medical condition was a drug-related chronic condition such as kidney disease, hepatitis C, or cirrhosis.

The county and state mental health and substance abuse professionals stated that while there may be HIPAA exceptions that allow the sharing of mental health or substance abuse patient information to other entities for the purposes of treatment, the patient's authorizing signature was still required. There was confusion over which policies, Federal or State, applied regarding the release of substance abuse information. Some of the discussion centered around a practice which states that even though the treatment center referred the homeless man to the shelter, the physician would not be authorized to re-release the patient's information back to the originating facility.

Some physicians in group and private practice shared that HIPAA allows them to have access to all of a patient's health information for the purpose of treatment. Others stated that while HIPAA allows the provider to have access to a patient's health information, they were aware that stricter laws regarding the exchange of substance abuse information would require them to obtain a release of information authorization from the patient or the patient's personal representative.

The physicians also reported that due to the stricter mental health and substance abuse laws, each of the three providers would need to obtain an authorization from the patient to share information with the other. Of concern to the physicians is the potential for the lack of continuity of care among the primary care physician, drug treatment center, and the specialist due to the disbursement of the patient's treatment records among three providers.

The stakeholders representing the substance abuse organizations stated that the well-established practices regarding the protection of a patient's substance abuse history which require the additional authorizations may be inconvenient to the providers but are appropriate. In the event of an emergent need for health information when a patient has a critical medical need, NC law supports the release of information without the patient's or legal representative's authorization.

Overall, the stakeholders were unaware of any legal barriers that would prohibit the providers from sharing information with each other. The stakeholders were unclear whether a homeless shelter is a facility or a HIPAA covered entity.

Scenario 17 Barriers
BR_7. Conflicting or outdated federal or state laws or regulations: The physicians and state employees identified policy barriers designed to protect the confidentiality of the patient's substance abuse history. However, they agreed that the policies were specifically tailored to safeguard this very sensitive information, so they deemed the barriers appropriate.

The LWG identified significant barriers to exchanging health information among multiple providers treating the same patient with a history of substance abuse. NCGS § 122C-55(i), the care and treatment exception to the prohibition against releasing without the patient's consent the health information of a mental health patient, states, "[u]pon specific request, a responsible professional may release confidential information to a physician or psych who referred the client to the facility." This statute allows the information to flow back to the referring provider(s), but it does not indicate how the provider can release the patient's information when he or she refers a client to an outpatient facility or other provider who did not refer the patient for the substance abuse treatment.

It is unclear why the statute is worded in a way that allows the provider to share the health information with the referring provider but not with another provider who subsequently treats the patient.

Scenario 18: Legal Compliance and Government Accountability

The Governor's office has expressed concern about compliance with immunization and lead screening requirements among low income children who do not receive consistent health care. The state agencies responsible for public health, child welfare and protective services, Medicaid services, and education are asked to share identifiable patient level health care data on an ongoing basis to determine if the children are getting the health care they need. Because of the complexity of the task, the Governor has asked each agency to provide these data to faculty at the state university medical campus who will design a system for integrating and analyzing the data.

Scenario 18 Stakeholder response
Due to the lack of stakeholder response, no information exchange practices were collected for this scenario.

Scenario 18 Barriers
None identified

Final Assessment of Variation Conclusions

Due to the quantity of barriers, limited resources, and time constraints, the NC HISPC project team identified proposed solutions for the top barriers that were vetted by the LWG, SWG, and Steering Committee. With additional time, continued resources and funding, North Carolina may consider further research into the barriers and potential solutions. Barriers and proposed solutions are grouped by categories of health information exchange, not ranked in order of priority.

Sub-Group 1 Patient Care Health Information Exchange

The VWG found that of the stakeholders who participated in the assessment sessions, the stakeholders who experienced the most significant variances in policy and business practices were the clinicians who practice independently or in a small group. These clinicians struggle to understand and appropriately interpret HIPAA's provisions due to lack of education, and they also typically lack workable technology needed to engage in secure and timely electronic health exchange. The VWG also found that clinicians are not hesitant to share patient information with other clinicians during emergencies but are apprehensive about sharing information for purposes other than direct treatment.

A significant barrier that interferes with the secure and timely exchange of health information is the scattered placement of an individual's health records and information. With the increase in specialty and alternative medicine, patients may seek multiple treatment options from different clinicians at several locations. Each clinician has a portion of the individual's health information and none of them benefit from having a complete set of information on the patient. In order to obtain more information about the patient, a majority of the clinicians send and receive extracts of the patient's records by fax or through verbal communication.

Another significant, if not alarming, barrier is the minimal adoption of electronic health records by North Carolina's clinicians. Clinicians indicate that their lack of health information technology adoption is due to the exorbitant costs of the systems, their mistrust of systems vendors, the unproven benefits of HIT adoption to patients and practices, their uncertainty over which vendor's technology to implement, and their fear of investing in outdated technology.

Clinicians in private practice usually would not require a patient's consent to use or release the patient's confidential medical information for the purposes of treatment, payment, or healthcare operations. However, depending on the manner in which physicians' legal counsel interpret NCGS § 8-53, such counsel may advise clinicians to obtain patients' consent before releasing patient health information, and to update such consent on an annual basis.

BR_7. Conflicting or outdated federal or state laws or regulations: NCGS § 8-53 Barrier to Release of Patient Information by the Physician Absent Patient Consent or a Court Order: This barrier arose in all scenarios. Although HIPAA states, "A covered healthcare provider may, without consent, use or disclose protected health information to carry out treatment, payment, or healthcare operations," (45 CFR § 164.506 (2)), NCGS § 8 – 53 may be interpreted to require the provider to obtain a consent in order to release the patient's confidential medical information for the purposes of treatment, payment, and healthcare operations. NCGS § 8 – 53 seems to be the State statute that most frequently arises as a legal barrier to the exchange of health information among health care stakeholders.

Sub-Group 2 Payment and PBM Health Information Exchange
Technological barriers between payers and individual and small physician groups delay the exchange of health information to process claims, and they continue to increase the administrative costs for the health care provider and payer.

Sub-Group 3 Secondary Use of Health Information
Marketing staff who participated in the assessment sessions stated that they are not required to participate in the hospital's HIPAA training. They state that since they don't deal with patient information, such training is not necessary; however, the LWG, health information security and IT staff believe that as

health information exchanges result in more complicated contractual agreements and technological solutions, having a privacy and security expert act as a “consultant” to the marketing staff during proposed marketing strategies would be beneficial to the organization.

The SWG realizes that as the implementation of health information technology becomes more prevalent, the information can be better protected from unauthorized attempts to access, modify, delete, or corrupt it. As health information security progresses to a model that is consumer controlled, people will have the opportunity to directly authorize the use of their health information for the purposes of operations, marketing, and research. Business models are being developed by the NHIN designers to address the secondary uses of health information for research and marketing and to incorporate appropriate privacy and security features tailored for such uses.

Sub-Group 4 Government Health Information Exchange

There are significant variances between NC statute, public policy, and actual practice among the policy makers and agency staff. Employees were well versed in their agency policies but cited confusion when they had to exchange information between state and county agencies. They stated that they would require authorizations from the individual before releasing information to another agency. This “consent overcompensation” requires an individual to sign additional authorizations to release information from county to state or agency to agency, even though HIPAA does not require an additional authorization.

Bioterrorism policies, law, and procedures continue to be under development by both the federal and state legislatures. This emerging area may be outside the realm of knowledge of this project team. Due to the project’s time constraints and limited resources, the NC HISPC project team recommends more awareness and training for this area as policy is developed and implemented.

As quality care and public health initiatives expand throughout North Carolina, significant technological barriers among physician groups or clinicians, clinics, rural hospitals, and county health departments prevent them from participating in state-sponsored quality initiatives and from reporting communicable diseases in a timely and accurate manner. Although North Carolina’s emergency rooms send information to the NC Public Health Information Network, the most utilized method of reporting a communicable disease from the clinician’s office is either by phone or fax to the local health department. As health information technology is adopted, such information would be readily available for epidemiological trending and forecasting.

Final Analysis of Solutions Report

Final Analysis of Solutions Report

Summary of Interim Assessment Variations

The objective of the first phase was to assess the variations in organization-level business policies and state laws that impedes health information exchange in North Carolina and its bordering states. The NC HISPC Variations Work Group (VWG) developed a simple assessment methodology to identify the stakeholders' current practices for sharing patient information, the reason for those practices, whether those practices caused any barriers to the exchange of health information, and whether any identified barriers were appropriate to safeguard the patient's information or were inappropriate.

The interviews and surveys from the assessment resulted in a vast collection of policies, procedures, barriers, and relevant state or federal laws which has been analyzed by the Legal and Solutions Work Groups.

The barriers have been grouped into three main barrier categories: policy, technological, and legal.

Of the approximately 75 business practices submitted, health information exchange barriers have been identified and categorized as followed:

BR_1. Range within organizations of misinterpretation and/or misapplication of laws or regulation
BR_2. Lack of business incentives to exchange information
BR_3. Lack of policy standardization across entities
BR_4. Lack of security standardization across entities
BR_5. Lack of interoperability between processes and technology
BR_6. Lack of workable technology
BR_7. Conflicting or outdated federal or state laws or regulations

In addition to the barriers identified by interviewees and the VWG, the SWG and LWG also found that some of the stakeholders' practices actually resulted in inappropriately withholding health information from the patient. The SWG and LWG discovered that release of information policies are designed to protect the clinician's or entity's liability rather than to support the consumer's right to privacy. Therefore, two additional barriers were added to address the issue of consumer empowerment. The consumer empowerment barriers are:

BR_8a. Lack of consumer understanding or awareness of the benefits of HIT, which results in lack of consumer input into the underlying policy and technology to support health information exchange
BR_8b. Lack of definition of consumer empowerment and lack of methodology for including it in policy and systems design

Analysis of Solutions Methodology

The NC HISPC Steering Committee (SC) developed a methodology that allowed team members to draw on their natural strengths, and that provided enough certainty for the PMO that the project would be completed within applicable deadlines.

Team members were constituted from responses to a call for volunteers that was included as part of the overall call for volunteers for the other NC HISPC groups. The Project Team was structured into four sub-groups that corresponded to four scenario clusters, each of which represented a general area of concern (*e.g.*, payer issues). Each sub-group member accepted a specialty role (*e.g.*, facilitator, writer, analyst, and researcher). This workgroup structure was accepted by the team members, the NC HISPC Steering Committee, and the Project Manager.

Team members came from a wide variety of health care entity stakeholders, including physician practices, hospitals, state government, consulting groups, academic medical centers, payers, quality improvement groups, and laboratories. The degree of involvement of each volunteer varied. Some

volunteers provided a significant number of hours, some provided a minimal amount of labor time, and others did not visibly participate. The agreed-upon work process was designed to function in this type of environment.

The Solutions Work Group (SWG) Chair, Dave Kirby, developed a work plan that included weekly goals to allow members to understand first the problems and issues, and then to formulate candidate solution outlines, followed by an opportunity to add commentary to those solution outlines that was then analyzed and commented upon by other project participants. This last element took the form of written sub-group reports. The work plan allowed each subgroup to work simultaneously. This design feature reduced the risk of missing the large project milestones because of a single group's delay. The plan called for the sub-groups to vet the various solutions and is structured to allow every viewpoint to be represented in the interim and final report along with group views of the applicability of each solution offered. This part of the plan anticipated an environment in which there was sufficient risk to each barrier and sufficient urgency in finding solutions, and that each offered solution would be pressed forward in some venue in NC at least to the point that it is field-tested. The Project Manager correlated and consolidated the various inputs and developed the report.

Each sub-group had access to a library of articles, provided by the NC HISPC Project Leadership, related to privacy and security in health data exchange. This briefing book was designed to aid their research. Members were urged to contribute additions to the book.

The SWG commentary on solutions in this report were vetted and prioritized by a consensus of the NC HISPC Steering Committee.

Solutions were organized by a characterization of the scope of the practice of information exchange to which each solution would apply, along with organizations that indicate the traits of various solutions related to historical issues of electronic health data exchange.

The feasibility of identified solutions was incorporated into the vetting process noted above. The process called for interested parties to comment on the drafts and have their comments included.

Analysis of Proposed Solutions

Each of our sub-groups has contributed solutions and solution elements along with analyses that relate to the scenario cluster that defined each group. The sub-groups are:

NC HISPC Scenario Sub-Group Work Clusters

Sub-group 1: Patient Care Scenarios	**Sub-group 2: Payer Scenarios**
1. Patient Care A (Emergency Transfer)	5. Payment (EHR Access)
2. Patient Care B (Substance Abuse)	9. Pharmacy Benefit A (Mail Order)
3. Patient Care C (Access Security)	10. Pharmacy Benefit B (Claims Savings)
4. Patient Care D (HIV and Genetics)	
Sub-group 3: Secondary Use Scenarios	**Sub-group 4: Government, Public Health & Safety Scenarios**
6. RHIO (Data Access)	13. Bioterrorism Event (Anthrax Spread)
7. Research (Data Usage)	15. Public Health A (Active TB Carrier)
8. Law Enforcement (Test Results)	16. Public Health B (Newborn Screening)
11. Operations and Marketing A (Rehab Center)	17. Public Health C (Homeless Shelters)
12. Operations and Marketing B (Birthing PHI)	18. Health Oversight (Legal Compliance)
14. Employment Information (Return to Work	

Each sub-group organized comments on their solutions per domain in textual form and in a tabular format. These are complemented by a synthesis of all of the sub-group solution proposals that makes apparent different and common traits. Each group also provided a list of key observations that should motivate future progress related to health information exchange in NC. This structure allowed the

emergence of a variety of ideas, illuminated useful comparisons among those ideas, and provides guidance for future work in this area.

The VWG, LWG, and SWG analyzed the barriers and proposed solutions to reduce or eliminate barriers that delay or prevent stakeholders from exchanging information with each other. Solutions are organized by a characterization of the scope of the practice of information exchange to which each solution would apply, along with organizations that indicated the traits of various solutions related to historical issues of electronic health data exchange.

The proposed solutions are not ranked in accordance to any particular order of priority:

SOL_1. Establish a pilot project with adequate funding to explore the concept of the Person-Oriented HIE.
SOL_2. Implement policy standards, such as model policy and legislation, to address the complexity and ambiguity surrounding the release of information.
SOL_2a. Implement security standards to address the complexity and ambiguity surrounding the safeguarding of health information.
SOL_3. Implement sound business models to incentivize potential information sharing partners to participate in community-based health information exchange.
SOL_4. Encourage greater collaboration between policy makers, subject matter, and technical experts to adopt HIE requirements.
SOL_5. Explore the dependencies between the business processes and their technical components for the purpose of interoperability.
SOL_6. Address the misinterpretation of laws or regulations by obtaining clarification and developing public and private awareness programs.
SOL_7. Amend conflicting federal or state laws.
SOL_8. Develop programs to raise awareness on the risks, benefits, and impacts of health information technology to a cross-section of consumers.

Proposed Policy Solutions

The SWG and LWG proposed key policy solutions intended to accelerate the adoption of health information technology, incentivize participation in community-based health information exchanges, encourage collaboration among stakeholders, explore dependencies between the business process and their technological component, and improve policy awareness.

HIT Adoption Incentives

As the age of health information exchange takes on new form throughout the United States, North Carolina's health care stakeholders should consider the advantages of adopting health information technology and participating in local, regional, and nationwide health information exchanges. In order to realize the objectives of the President's vision for the development and implementation of a nationwide interoperable health information technology infrastructure designed to improve the quality, safety, and efficiency of health care and the ability of most consumers to have electronic health records (EHR) by 2014, the adoption of EHRs must increase substantially from the 23% implementation rate that was announced during the 2007 HIMSS National Conference.

In follow-up discussions with the Variations Work Group, government agencies, facilities, and providers in North Carolina, all indicated that the most significant barriers to sharing heath information electronically with another entity were their fear of non-compliance with HIPAA and their lack of electronic technology. Less than 25% of health care facilities and providers have adopted EHRs, making participation in local, regional, or nationwide health information exchanges less of a priority. Among the reasons for not investing in EHRs are a mistrust of software vendors, confusion over which technology(ies) to adopt, lack of IT staff to support a system, integration of EHRs into other systems and handheld devices, and concerns about usability of the EHRs for staff. Two additional reported reasons that were frequently cited are the high costs of the new technology(ies) and the lack of convincing evidence on the benefits of

EHRs. North Carolina HISPC recommends numerous strategies to encourage the adoption of health information technology and participation in health information exchanges.

Proposed Solution(s)

US Senate Bill S 628, "Critical Access to Health Information Technology Act of 2007," authorized the appropriation of ten million dollars to improve access to health care in rural areas by improving technology. Under this program, North Carolina could be eligible for up to $250,000 to be distributed among the State's 24 critical access hospitals.

NC HISPC recommends that the NC Hospital Association and the NC Department of Health and Human Services apply for this grant and seek additional sources of funding, such as matching awards, to offset the often underestimated costs to companies of the business process changes required by new technology. The additional funding could be utilized to conduct privacy and security gap analyses, provide HIPAA awareness training for health industry stakeholders and the general public, map business processes and patient flow to its technological component, and implement training for IT staff in the areas of privacy, security, and technical support.

In addition to providing health care information technology funding for North Carolina's critical access hospitals, the NC HISPC team also recommends similar programs for individual and group health care practices and facilities.

Finally, the team recommends a mechanism such as an annual study,, perhaps sponsored by the NC Attorney General's Consumer Protection Division, to analyze features, costs, benefits, customer satisfaction, current implementations, CCHIT status, and other similar criteria for EHRs that would equip the potential EHR adopters and funders with the knowledge necessary to make informed decisions on HIT purchases.

Rationale:

Supplementing the health care providers' and facilities' investment in health information technology will reduce the cost barriers to adoption.

Currently there is mistrust between providers and vendors of HIT products. This mistrust is rooted in the mergers and acquisitions of healthcare's leading information systems vendors during the mid-1990s, which resulted in the "sunsetting" of many hospital information systems, as well as in the perceived urgent need to resolve the systems date change for the year 2000. As consumers of health information technology, stakeholders in the health care community began experiencing a paradigm shift in which they perceived the vendor and its technology as controlling the direction of their health care practice. This sense of loss of control became especially prominent when providers were required to comply with HIPAA transactions and its implied application security; however, the solution, as in the case of Y2K, was controlled by the application software vendor, who in many cases was able to over promise about the effectiveness of the technology because the provider had to purchase some version of that technology in order to continue to submit claims. Membership grew in systems users groups and other organizations that allowed the stakeholders to convene and learn about new trends in HIT, participate in studies of their EHR implementations, and advocate for application systems standards.

The above proposed solutions of supplemental information technology adoption and annual studies of HIT benefits are designed to empower health care providers and facilities with sufficient knowledge to make informed decisions about the features and benefits of HIT applications and to build incentive strategies for implementing those applications.

HIE barrier addressed: Lack of business incentives to exchange information; Lack of interoperability between processes and technology; Lack of workable technology

HIE type: 1. Direct Patient Care; 2. Payer; 3. Secondary Use: Operations, Marketing, Research, Law Enforcement; 4. State Government / Public Health

HIE model affected: 1. E2E – Entity to Entity; 2. PO HIE – Person Oriented Health Information Exchange

Applicability of solution: Consumers, providers, and potential funders

Stakeholders affected (1 – 18):
1. Clinicians
2. Physician Groups
3. Federal Health Facilities
4. Hospitals
5. Payers
6. Public health agencies
7. Community clinics and health centers
8. Laboratories
9. Pharmacies
10. Long term care facilities and nursing homes
11. Homecare and hospice
14. Medical; public health schools; research
15. Quality improvement organizations
16. Consumers or consumer organizations
17. State government

Privacy & security domain (s) addressed (1 – 9):

Domains	
1. Authentication	X
2. Authorization	X
3. Identity Matching	X
4. Transmission	X
5. Integrity	X
6. Event Audit	X
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues:
Worker anxiety and interruption of business flow are common outcomes during implementation of new technologies. Programs to address the organization's training needs and resultant cultural changes should be included in the implementation.

HIE Participation Incentives

The second initial key finding is that there often is a lack of business motivation or incentive to carry out appropriate routine electronic health information flow. Business incentive to carry out many exchanges is low enough that almost any barrier (de minimus liability, minor labor costs, small transaction friction) will nonetheless be high enough to deter appropriate and routine health data exchange. Although addressing business barriers which are largely unrelated to privacy and security concerns is beyond the direct scope of this project, for privacy/security solutions to be useful they must at least not increase these business barriers and should ideally lower them and offer support to other broad health-related goals.

Although funding the adoption of health information technology will partially address the cost barriers cited by the stakeholders, there remains a lack of incentive to share information with other entities. The stakeholders admitted to guarding health care information even "from" the person who is the subject of the information. They did so out of concern that the information could be used against the stakeholder or

that the health information is incomplete or disparately-maintained. Stakeholders' biggest concern about sharing health information was that they might lose patients to another provider, facility, or health plan.

Consumers, on the other hand, reported that they thought their health care information already was being exchanged among their different health care providers. Consumers were confused about why they had to sign so many forms to release their health information or obtain copies of that information for themselves. They often experienced delays in obtaining referral or diagnostic appointments because they were missing an order or a report. The consumers also noted that even though their health information didn't always make it to the appropriate place in a timely manner, they received invoices and statements from the health plan, facilities, and providers seamlessly.

Does that imply that the current incentive to share information is financially-based? The VWG and LWG concurred that the liability and competitive reasons for not sharing are stronger than incentives to share. The LWG and SWG found that given all of the complexities of our fragmented health care system (lack of workable technology, conflicting state and federal laws), proposing incentives for information sharing was an abstract exercise. Although the VWG, LWG, and SWG were able to identify a direct barrier to exchanging health information (lack of incentive to share), they do not believe that a policy, legal, or regulatory solution would eliminate or reduce the barrier. The stakeholders' lack of incentive to participate in health information exchanges is a systemic health care design issue that must be studied further.

Although addressing business models is beyond the scope of the HISPC project, at the same time, developing a valid business model for information sharing is vital to ensuring that our country maintains a sustainable system of quality health care delivery. As such, the NC HISPC team proposes further exploration of health care delivery models.

Proposed solution(s): Explore sound business models to incentivize potential information-sharing partners to participate in community-based health information exchange.

Rationale for Solution:

Through the application of data standardization, security practices, and transmission protocols, a successful demonstration of interoperable electronic health information exchanges was exhibited at the recent NHIN forum in January 2007. The NC HISPC project has successfully identified many of the policy and legal barriers to exchanging health information in North Carolina, and it has proposed solutions to reduce or eliminate these barriers. However, the NC HISPC team is concerned that building an expensive technologically-based health care system, without first evaluating the underlying financial models available to sustain such a system, could result in a failed system, such as the recent experience of the Santa Barbara County Health Data Exchange (CA).

Before North Carolina begins to build community-based health information exchanges, it should first consider identifying and studying viable financial models in order to ensure that the information exchanges are sustainable. A comparative study of the current reimbursement model of health care delivery and several value-driven outcomes-based models would provide policy makers from government-sponsored health care programs, health plans, and the medical community more of the information they need either to develop new, or expand upon current, financial-quality models.

In their March 14, 2007 article in the *Journal of the American Medical Association*, Drs. Porter and Teisberg emphasized that the "purpose of the health care system is not to minimize costs, but to deliver value to patients, better health per dollar spent." They noted that in a quality-centered health care system, providers are rewarded for improved outcomes, health plans (public and private) contain costs, and patients receive better care. Their model system focuses on the interrelated medical needs of the person rather than on reimbursing through episodic visits or practice specialties. They attempt to address the reduction of the practitioner's "dysfunctional competition" through interdependent treatment practices for certain medical conditions.

The Porter-Teisburg quality-driven model is just one example which North Carolina thought leaders might explore. North Carolina has resources in its large rural health communities, public and private health plans, malpractice professionals, research and economics experts, and public policy makers. Leveraging all these resources to compare existing and new health care delivery models would align all these stakeholders and focus them on achieving the same, mutually-desirable goal—that of better quality, more cost-effective care.

HIE barrier addressed: Range within organizations of misinterpretation and/or misapplication of laws or regulation; Lack of incentives to exchange information; Lack of interoperability between processes and technology; Lack of workable technology

HIE type: 1. Direct Patient Care; 2. Payer; 3. Secondary Use: Operations, Marketing, Research, Law Enforcement; 4. State Government / Public Health

HIE model affected: 1. E2E – Entity to Entity; 2. PO HIE – Person Oriented Health Information Exchange

Applicability of solution: Consumers, providers, and potential funders

Stakeholders affected (1 – 18):
1. Clinicians
2. Physician Groups
3. Federal Health Facilities
4. Hospitals
5. Payers
6. Public health agencies
7. Community clinics and health centers
8. Laboratories
9. Pharmacies
10. Long term care facilities and nursing homes
11. Homecare and hospice
14. Medical; public health schools; research
15. Quality improvement organizations
16. Consumers or consumer organizations
17. State government

Privacy & security domain (s) addressed (1 – 9):

Domains	
1. Authentication	X
2. Authorization	X
3. Identity Matching	X
4. Transmission	X
5. Integrity	X
6. Event Audit	X
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues:
Providers have expressed concerns over losing patients to other providers.

Encourage Collaboration

Building a framework to exchange health information, from consumer to provider and entity to entity, requires a new approach in policy development and systems design. Before North Carolina considers funding large-scale technological initiatives, the NC HISPC team recommends that the North Carolina General Assembly establish and fund a task force to address the interoperability challenges faced by health care stakeholders who desire to participate in local, state, and nation-wide health information exchanges such as RHIOs or the Nationwide Health Information Network.

Other states, such as Florida and West Virginia, have established a formal independent body to oversee the planning and implementation of the HIT initiatives in their states. In 2004, Florida Governor Jeb Bush's Executive Order Number 04-93 established the Governor's Health Information Infrastructure Advisory Board. The Advisory Board, consisting of health care policy and information technology experts and representatives from the provider community, advises the Agency for Healthcare Administration (NC DHHS' equivalent) as Florida develops and implements a strategy for the adoption and use of electronic health records.

Proposed solution(s):
Encourage greater collaboration among policy makers, subject matter, and technical experts to adopt HIE requirements.

Rationale for Solution:
North Carolina has participated in several HIT collaborative projects in many areas of the state when there was an incentive to do so, such as HIPAA compliance or a remunerative business arrangement.. However, the methodologies and tools used in those projects are subject to proprietary protections of the companies that developed them, so the knowledge gained and tools used generally are not available to other health care stakeholders interested in participating in HIE exchange. Developing information sharing agreements, project tools, training, and implementation plans is very costly and also requires specific skill sets of subject matter experts who usually are not employed by small- to mid-level health care stakeholders. The establishment of an infrastructure task force, under the leadership of the State of North Carolina, might build public policy and technical infrastructure in conjunction with one another. Stakeholders also would benefit from open forums so that they could apply researched and tested methods in their individual HIE planning and implementations.

HIE barrier addressed:
Lack of interoperability between processes and technology

HIE type (Groups 1 – 4): 1. Direct Patient Care; 2. Payer; 4. State Government / Public Health

HIE model affected (E2E, PCHDX): 1. E2E – Entity to Entity, 2. PO HIE – Person Oriented Health Information Exchange

Applicability of solution: The senders and receivers of health information.

Stakeholders affected (1 – 18): All

Privacy & security domain (s) addressed (1 – 9):

Domains	
1. Authentication	X
2. Authorization	X
3. Identity Matching	X
4. Transmission	X
5. Integrity	X
6. Event Audit	X
7. Safeguards	X

8. Data classification	X
9. Policies	X

Potential barriers / issues:
With the NC General Assembly adjourning in late April, there is no time to seek a sponsor and include this concept in this session's agenda.

Explore Process - Technological Dependencies

Background:
Overcoming privacy, security, and other barriers to the routine exchange of electronic health information involves finding ways to interconnect the business and technical processes related to the information exchange. For example, finding a way to ensure that two entities, such as a provider and a health plan, have the same person in mind (identity matching) before they exchange health information about that person requires technical and business process similarities.

Integrating the HIPAA transactions and code set data element mapping processes with generally accepted information security risk management methodologies could assist information privacy and security professionals with the adoption of standard risk management practices.

Proposed solution (s):

SOL_5. Explore the dependencies between the business processes and their technical components for the purpose of interoperability. Create models for internal business practices to be used in combination with standards of other organizations.

Rationale for Solution(s):

During the remediation of HIPAA electronic transactions, the process employed by information systems developers included the identification and documentation of the health care payment process, the development of business flow diagrams, and mapping the proprietary data elements of their systems to the required X12 standards, then developing software programs to convert the propriety data elements into X12 format. A "data dictionary" containing the definitions and representations of the data elements is either generated by the database management system or created by systems professionals.

A similar methodology during the remediation of HIPAA privacy and security required covered entities to identify individually identifiable information and categorize the protected health information (PHI) by type (demographic, financial, clinical), level of sensitivity to the subject of the information in the event of a wrongful disclosure or security breach, and criticality if it becomes unavailable, modified, or damaged.

Integrating the information gathered from mapping the transactions and code sets and the categorization, sensitivity, and criticality of PHI would give health care analysts and systems engineers an initial determination of the business processes and their correlating technological components. The knowledge base can be expanded and shared with the Health Information Technology Standards Panel (HITSP) that is charged to develop a widely-accepted and useful set of standards to enable and support interoperability among health care software applications. By collaborating with HITSP, North Carolina health care stakeholders can assist in the acceleration of health information interoperability.

HIE barrier addressed: Lack of interoperability between processes and technology

HIE type (Groups 1 – 4): 1. Direct Patient Care; 2. Payer; 3. Secondary Use: Operations, Marketing, Research, Law Enforcement; 4. State Government / Public Health

HIE model affected (E2E, PCHDX): 1. E2E – Entity to Entity, 2. PO HIE – Person Oriented Health Information Exchange

Applicability of solution: The senders and receivers of health information.

Stakeholders affected (1 – 18): All

Privacy & security domain (s) addressed (1 – 9):

Domains	
1. Authentication	X
2. Authorization	X
3. Identity Matching	
4. Transmission	X
5. Integrity	X
6. Event Audit	X
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues: Process flows are labor intensive and costly.

Improve Policy Awareness

From organization to organization, there is a broad range in the manner in which laws related to appropriate use and disclosure of information are interpreted and applied. The LWG attributed this finding to a lack of understanding or education about the law (and a consequent need for such education to be provided), as well as to the possible need for a formal legal clarification or amendment.

In addition to suggesting potential revisions to the North Carolina General Statutes and Administrative Code to align state law restrictions on release of information with existing federal restrictions, the NC HISPC Team recommends that North Carolina emphasize education about appropriate release of information for all entities involved in the exchange of health care information – including providers, payers, vendors, and consultants – to ensure that both requestors and releasers of information are familiar with the circumstances under which health information may be used and released.

Employees often are not aware of their employer's policies or procedures related to appropriate uses and disclosures of health information. For this reason, health care industry stakeholders must train employees on such appropriate uses and releases, both now and following any revisions to State or Federal laws regarding appropriate uses and releases of health information. The proposed Internet repository also might be expanded to assist in this regard.

Solution: Address the misinterpretation of laws or regulations by obtaining clarification and developing public and private awareness programs.

Rationale for Solution:
Health care stakeholders already regularly provide to their employees legally mandated training on topics such as blood borne pathogens, reportable diseases, and OSHA. A HIPAA and North Carolina law training program that employers require their employees to attend could reduce the misapplication of health information privacy and security standards in North Carolina's health care industry.

HIE barrier(s) addressed: Range within organizations of misinterpretation and/or misapplication of laws or regulation

HIE type: 1. Direct Patient Care; 2. Payer; 3. Secondary Use: Operations, Marketing, Research, Law Enforcement; 4. State Government / Public Health

HIE model affected: 1. E2E – Entity to Entity; 2. PO HIE – Person Oriented Health Information Exchange

Applicability of solution: Covered entities under HIPAA

Stakeholders affected (1 – 18): All

Privacy & security domain (s) addressed (1 – 9:

Domains	
1. Authentication	X
2. Authorization	X
3. Identity Matching	X
4. Transmission	X
5. Integrity	X
6. Event Audit	X
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues:
Opposition to specific changes is possible.

Proposed Legal Solutions

In addition to the identified business, technology, and consumer barriers to health information exchange, there were identified significant legal barriers that should be brought to the attention of the General Assembly.

The first, which applied to all levels of health information exchange, is NCGS § 8 – 53, a North Carolina statute that establishes the physician-patient privilege, which protects information patients share with their physicians from release to third parties without the patient's consent or a court order. This state statute was designed originally to encourage patients to share freely their health care information with physicians. This law states, "No person, duly authorized to practice physic or surgery, shall be required to disclose any information which he may have acquired in attending a patient in a professional character, and which information was necessary to enable him to prescribe for such patient as a physician, or to do any act for him as a surgeon, and no such information shall be considered public records under G.S. 132-1. Confidential information obtained in medical records shall be furnished only on the authorization of the patient, or if deceased, the executor, administrator, or, in the case of unadministered estates, the next of kin." However, the HIPAA Privacy Rule states, "A covered healthcare provider may, without consent, use or disclose protected health information to carry out treatment, payment, or healthcare operations," 45 CFR § 164.506 (2).

Generally, NCGS § 8 – 53 has been interpreted as requiring the physician to obtain a patient's consent before releasing the patient's health information for purposes of treatment, payment, and healthcare operations. It seems to be the state statute that most frequently acts as a legal barrier to the exchange of health information among health care stakeholders for treatment and operations. Virtually all providers who perform third-party billing functions get prior written consent for sharing information needed for payment.

Second, the federal Clinical Laboratory Improvement Amendments of 1988 ("CLIA") regulations currently provide that "Test results must be released only to authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test." 42 CFR §

493.1291(f). The term "authorized person" is defined in 42 CFR § 493.2 as "an individual authorized under State law to order tests or receive test results, or both." The term "individual responsible for using the test results" is not defined in the CLIA regulations, and there is considerable uncertainty as to its meaning.

These CLIA provisions pose barriers to laboratories exchanging health care information directly with non-ordering providers to whom the patient is referred, with RHIOs, or with other stakeholders who may desire to participate in electronic health information exchange for legitimate purposes otherwise permitted by HIPAA, but who are not identified as "authorized persons" for the receipt of test results under State law.

The legal solutions section of this report presents the vetted recommendations for reducing the legal obstacles to exchanging health information that were identified in the Variation of Assessment Report. It should be noted that the LWG recommendations are not to be considered authoritative work on behalf of the North Carolina General Assembly.

Model Legislative Solutions

Providers are apprehensive about sharing health information with patients or others legitimately requesting that information based upon their fear of potential liability for inappropriately releasing such information and competitive interests that cause providers to refrain from sharing such information, among other things.

Comments from the Variations phase of this project indicate that providers view many instances of information release as unacceptably risky, in part because the policies related to such releases are too complex and/or vague for the typical releaser to be confident that he or she has correctly interpreted such policies. Therefore, solutions are needed to address the complexity and ambiguity of the current rule set for releasing information. Two proposed solutions have dominated the work to date: (1) simplify the rule set (at least from the releaser's point of view) without increasing the risk of a privacy breach or eliminating releases that patients want to occur; and (2) improve the level of training about the rule set for health information releasers and requestors.

Solution: Implement policy standards, such as model policy and legislation, to address the complexity and ambiguity surrounding the release of information. The LWG discussed a variety of potential solutions, including: (1) Have the National Conference of Commissioners on Uniform State Laws (NCUSL) create model consent forms that all states may adopt; (2) Create a safe harbor that protects any person or entity who in good faith releases protected health information for purposes of treatment; (3) Recodify all North Carolina statutes and regulations relating to release of patient health information in one or more consecutive sections within the General Statutes and the Administrative Code for ease of reference; (4) Alternatively, create an official compendium of state statutes and regulations that address confidentiality and release of patient health information, and make the compendium available to health care stakeholders; (5) Specifically for disease reporting and other legally required health information reporting, initiate an Internet repository of directions for health care providers that will answer questions as to who is responsible for reporting what health care information, to whom reports must be made, the periodicity of such reports, and the appropriate reporting mechanism(s), and provide appropriate training on how to access and use the repository; and (6) Create new legislation to protect the privacy of health information in electronic form and to address the circumstances under which release of such information is appropriate, including for purposes of telemedicine and e-prescribing, and potentially specifically state that this new law supersedes current laws and regulations regarding exchange of information in the paper context.

HIE barrier(s) addressed: BR_1. Range within organizations of misinterpretation and/or application of laws or regulation; BR_3. Lack of policy standardization across entities; BR_5. Lack of interoperability between processes and technology; BR_7. Conflicting or outdated federal or state laws or regulations.

HIE type: 1. Direct Patient Care; 2. Payer; 3. Secondary Use: Operations, Marketing, Research, Law Enforcement; 4. State Government / Public Health

HIE model affected (E2E, PO HIE): 1. E2E – Entity to Entity, 2. PO HIE – Person Oriented Health Information Exchange

Applicability of solution: Public policy makers

Stakeholders affected (1 – 18): ALL

Privacy & security domain (s) addressed (1 – 9): Review the domains description. Populate the domains table this solution addresses.

Domains	
1. Authentication	X
2. Authorization	X
3. Identity Matching	X
4. Transmission	X
5. Integrity	X
6. Event Audit	X
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues:

Consumers would need to accept that their right to consent to releases of their health information must be subject to exceptions for disclosures for purposes of protecting the public health, emergency treatment, and the uses and disclosures of health information that do not require authorization for release.

Model Policy Solutions – RHIO and HIE

Background: There is confusion in the marketplace about what exactly a RHIO or a HIN is and, therefore, what privacy and security protections must exist in order for appropriately protected information exchange within a RHIO or HIN.

Solution: Adopt generally accepted models and terms when referring to regional health information exchange organizations (or RHIOs), health information networks (or HINs), or similar entities that engage in electronic health information exchange. We need to have and use a standardized set of definitions and terminology to assure health care literacy, HIT literacy, and accuracy of information based on the data provided.

Rationale for Solution: Standardizing terminology and definitions, along with identifying the different "corporate" models of RHIOs and HIEs, should assist the health care industry by improving awareness and understanding of the various options for health information exchange going forward.

HIE barrier(s) addressed: BR_1. Range within organizations of misinterpretation and/or application of laws or regulation; BR_2. Lack of business incentives to exchange information; BR_3. Lack of policy standardization across entities; BR_4. Lack of security standardization across entities; BR_5. Lack of interoperability between processes and technology; BR_7. Conflicting or outdated federal or state laws or regulations.

HIE type (Groups 1 – 4): 1. Direct Patient Care; 2. Payer; 3. Secondary Use: Operations, Marketing, Research, Law Enforcement; 4. State Government / Public Health

HIE model affected (E2E, PO HIE): 1. E2E – Entity to Entity; 2. PO HIE – Person Oriented Health Information Exchange

Applicability of solution: North Carolina General Assembly, NHIN and RHIO participants

Stakeholders affected (1 – 18): ALL

Privacy & security domain (s) addressed (1 – 9): Review the domains description. Populate the domains table this solution addresses.

Domains	
1. Authentication	X
2. Authorization	X
3. Identity Matching	X
4. Transmission	X
5. Integrity	X
6. Event Audit	X
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues: Opposition to specific changes is possible.

Proposed State Law Solutions for North Carolina

Recodifying North Carolina Statutes

Background: Currently, laws and regulations pertaining to the confidentiality of health information and the circumstances under which release of such information is and is not appropriate are found in several sections of the North Carolina General Statutes and the North Carolina Administrative Code, including the evidence section, the juvenile code, the insurance section, the mental health and substance abuse section, and the public health section, to name just a few. This creates a fragmented maze of protections, each of which was written based upon the interests and needs of a particular subset of persons who may have access to health information. This maze is difficult to navigate and the fragmentation makes it difficult to quickly and accurately determine whether particular releases of health information are appropriate or not in given circumstances. Attorneys, health care consultants, and health care providers alike acknowledge that the current organization of release of information laws in North Carolina serves as a barrier to timely and appropriate exchange of health care information.

Solution: Either **recodify** the state's health care-related statutes and regulations so that all statutes and regulations regarding release of health care information may be found within a single section or several consecutive sections of the General Statutes and the Administrative Code, or create an official compendium of state statutes and regulations that addresses confidentiality and release of patient health information and that can be provided to health care stakeholders for easy reference.

Rationale for Solution: When stakeholders can more easily determine whether it is appropriate for them to release health information, they will be more likely to participate in appropriate health information exchange because the fear of liability for inappropriate releases should be diminished.

HIE barrier(s) addressed: BR_1. Range within organizations of misinterpretation and/or application of laws or regulation; BR_3. Lack of policy standardization across entities; BR_4. Lack of security standardization across entities; BR_5. Lack of interoperability between processes and technology BR_7. Conflicting or outdated federal or state laws or regulations.

HIE type (Groups 1 – 4): 1. Direct Patient Care; 2. Payer; 3. Secondary Use: Operations, Marketing, Research, Law Enforcement; 4. State Government / Public Health

HIE model affected (E2E, PO HIE): 1. E2E – Entity to Entity, 2. PO HIE – Person Oriented Health Information Exchange

Applicability of solution: North Carolina General Assembly

Stakeholders affected (1 – 18): All health care stakeholders

Privacy & security domain (s) addressed (1 – 9):

Domains	
1. Authentication	
2. Authorization	
3. Identity Matching	
4. Transmission	
5. Integrity	
6. Event Audit	
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues: Recodifying will be extremely time-consuming and a practical challenge, and special interests (*e.g.*, insurance industry, mental health industry) may prefer to have release of information laws and regulations related to their industry maintained where they are now.

Expand Public Health Reporting
Chapter 10A of the North Carolina Administrative Code contains several chapters in which specific regulations require the reporting of diseases to various state oversight agencies. Once again, because of this fragmented maze of requirements, health care providers often do not know that they have an obligation to report certain information.

Solution: We need to expand communicable disease and bio-surveillance reporting beyond North Carolina's emergency room. Recodify the administrative code sections on disease reporting, or prepare a compendium of all the requirements, and make this compendium available to all health care providers. Alternatively, initiate an Internet repository of directions for providers that will answer questions as to who is responsible for reporting what information, to whom reports must be made, the periodicity of such reports, and the appropriate reporting mechanism(s). Training must be offered to all persons or entities required to make reports regarding where to find the repository and how to use it.

Rationale for Solution: Clarification of the public health and disease reporting requirements and providing easy access to those requirements, as well as providing a format for asking questions about reporting responsibilities, should increase compliance with reporting requirements and improve the accuracy of North Carolina's disease registries.

Amend NCGS § 122C-55(i)

NCGS § 122C-55. Re-disclosure of Mental Health Information.

Original text:
Subsection (i) "Upon specific request, a responsible professional may release confidential information to a physician or psychologist who referred the client to the facility."

NCGS § 122C-55(i) allows for release of mental health and substance abuse information without patient authorization to the physician or psychologist who referred a patient to the facility, ***but it fails to provide***

for release of this information without authorization to any other physician who currently is treating the patient (such as a primary care provider or specialist) or who treats the patient in the future. This prohibition on sharing information for treatment purposes unless the patient authorizes the release hinders the provision of patient care – both mental health and substance abuse treatment and physical medical care.

Solution:
Amend NCGS § 122C-55(i) to permit, without patient authorization, disclosure of mental health or substance abuse information to any provider who is treating the patient, either mentally or physically.

Rationale for Solution:

The original language was developed before health care delivery became integrated and physical health and behavioral health became accepted as inter-dependent variables of a person's total health care. The two systems were isolated, with behavioral health viewed more as "social services" and acute/physical health viewed as "health;" now they both are viewed as important components of a person's "health," and the data validates that treatment or failure of treatment of one component affects the other. In addition, the language was written before the expansive use of pharmaceuticals in non-institutional settings; the new, broader use of pharmaceuticals requires knowledge by both physical and mental health providers of what the other provider has prescribed and the consumer has taken. Finally, the original language was written when individuals with major mental health and chemical use problems were institutionalized; as these individuals all were part of an enclosed system, the previously noted issue did not exist. Today, it is a significant issue in many patients' health care.

Amending NCGS § 122C-55(i) will allow a mental health provider to provide crucial patient information to a subsequent or concurrent provider of mental or physical health care. In some instances, a mental health patient is unable or unwilling to share his/her information, but sharing the information may be vital to the effective treatment of the individual. By allowing this information to be shared for treatment purposes, just like physical health information would be shared, care can be provided more efficiently and effectively. The effectiveness of any amendment, however, may depend upon revision to the federal regulations regarding substance abuse treatment information, addressed below (42 CFR §§ 2.1 and 2.2).

HIE barrier(s) addressed:
BR_1. Range within organizations of misinterpretation and/or application of laws or regulation
BR_3. Lack of policy standardization across entities
BR_4. Lack of security standardization across entities
BR_5. Lack of interoperability between processes and technology
BR_7. Conflicting or outdated federal or state laws or regulations.

HIE type: 1. Direct Patient Care; 4. State Government / Public Health

HIE model affected: 1. E2E – Entity to Entity; 2. PO HIE – Person Oriented Health Information Exchange

Applicability of solution: Mental health providers, North Carolina General Assembly, North Carolina Department of Mental Health and Substance Abuse

Stakeholders affected (1 – 18):
1. Clinicians
2. Physician Groups
3. Federal Health Facilities
4. Hospitals
6. Public health agencies
7. Community clinics and health centers
10. Long term care facilities and nursing homes
11. Homecare and hospice
16. Consumers or consumer organizations

17. State government

Privacy & security domain (s) addressed (1 – 9:

Domains	
1. Authentication	
2. Authorization	X
3. Identity Matching	
4. Transmission	
5. Integrity	
6. Event Audit	
7. Safeguards	
8. Data classification	X
9. Policies	X

Potential barriers / issues: Opposition to specific changes is possible.
Clients may object to additional individuals receiving their mental health information when, in some instances, they don't approve certain subsequent providers.

Proposed Federal Law Solutions

42 CFR §§ 2.1 and 2.2

Background:

For release or re-release of substance abuse treatment information to third parties, federal law requires patient authorization or a court order, and it further requires the releasing party to provide notice of these restrictions upon any re-disclosure of such information so that any party accessing this information must observe these restrictions (42 CFR § 2.32).

For facilities that receive federal funding, 42 CFR §§ 2.1 and 2.2 pre-empt NCGS § 122C-55(i). Substance abuse information is specially protected, so a consent for release must specify release of this information. Some hospitals include a space on their general consent forms for patients to initial in the event that the patient agrees to allow the hospital to release health information regarding the patient's substance abuse. Because substance abuse information is specially protected, it also needs to be segregated in the medical record in order to maintain such special protection, whether the record is maintained in paper or electronic format. Some facilities have policies specifying that substance abuse information must be maintained separately in the patient's medical record.

Solution: Amend 42 CFR §§ 2.1 and 2.2, the Federal substance abuse treatment provisions, to allow for re-release of such information to health care providers without limitation for the purpose of treatment.

Rationale for Solution: Due to the requirements within 42 CFR §§ 2.1 and 2.2 for additional authorization from the patient to re-disclose substance abuse treatment information, the treating physician often may treat the patient with incomplete information (*i.e.*, without knowledge that the patient has been or is in treatment for substance abuse). This creates a risk of harm to the patient. Although this sensitive information generally should be protected, treating providers need access to this information in order to make appropriate treatment and drug interaction determinations for the patient.

HIE barrier(s) addressed: BR_1. Range within organizations of misinterpretation and/or application of laws or regulation; BR_3. Lack of policy standardization across entities; BR_4. Lack of security standardization across entities; BR_7. Conflicting or outdated federal or state laws or regulations. BR_8a. Lack consumer input into the design of policy and technology; BR_8b. Lack of definition of consumer empowerment and methodology to its inclusion in policy and systems design

HIE type (Groups 1 – 4): 1. Direct Patient Care; 2. Payer; 4. State Government / Public Health

HIE model affected (E2E, PO HIE): 1. E2E – Entity to Entity; 2. PO HIE – Person Oriented Health Information Exchange

Applicability of solution: Mental Health (including substance abuse) stakeholders including providers, facilities, government, and individuals seeking treatment

Stakeholders affected (1 – 18):
1. Clinicians
2. Physician Groups
3. Federal Health Facilities
4. Hospitals
5. Payers
6. Public health agencies
7. Community clinics and health centers
10. Long term care facilities and nursing homes
11. Homecare and hospice
14. Medical; public health schools; research
16. Consumers or consumer organizations
17. State government

Privacy & security domain (s) addressed (1 – 9):

Domains	
1. Authentication	
2. Authorization	X
3. Identity Matching	X
4. Transmission	
5. Integrity	
6. Event Audit	
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues: Complicated federal and state mental health laws may deter participation. In addition, lack of understanding about the patient care consequences of the current law, as well as concern about the sensitivity of this information, may spark disagreement among substance abuse/mental health patient advocates about these proposed solutions.

Proposed CLIA Amendment

Clinical laboratories face significant regulatory obstacles in delivering test results to persons other than the physician or other authorized person who ordered the test, even when the requests for such results are for legitimate purposes in furtherance of consensus public policy objectives such as quality improvement, disease management, patient safety, elimination of duplicative testing, and reducing health care costs. The successful achievement of these policy goals will depend upon the ability of laboratories to deliver both real-time and historical test results to persons who are in many cases not currently authorized to receive them under existing law. These difficulties arise primarily from regulations promulgated under the Clinical Laboratory Improvement Amendments of 1988 ("CLIA") and State law.

Under the CLIA regulations, 42 CFR § 493.1291(f) currently provides that "Test results must be released only to authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test." The term "authorized person" is defined in 42 CFR § 493.2 as "an individual authorized under State law to order tests or receive test results, or both." The term "individual responsible for using the test results" is not defined in the CLIA regulations, and there is considerable uncertainty as to its meaning.

CLIA's deference to State law for purposes of determining the permissible recipients of laboratory results is problematic because many State laws very narrowly proscribe those persons who are authorized to order tests or receive test results, and variation among State laws has created a patchwork of different standards. For example, in Arizona, the result of a test must be reported to the person who authorized it, and those authorized persons are limited to podiatrists, chiropractors, dentists, physicians, or a person licensed to practice medicine in another state. A.R.S. § 370-40 (A) and (B). In Georgia, test results must be reported only to, or as directed by, a licensed physician, dentist, or other authorized person requesting the test. GA Rules & Regulations § 290-9-8-.25. In North Carolina, there is an absence of state law specifically addressing the issue of who is authorized to receive test results, so under CLIA, only those who are authorized to order tests under North Carolina law are authorized to receive results. Persons or entities that are not expressly identified in these typical provisions include non-ordering physician specialists to whom a patient has been referred by a primary care physician, Regional Health Information Organizations (RHIOs), quality improvement organizations, disease management companies, health plans, and even CMS, all of whom are seeking lab result data for legitimate purposes. While in many states labs are permitted to deliver test results to persons or entities authorized by the ordering physician to receive them, obtaining or confirming such authorization is often very impractical.

Background

We are proposing three alternative regulatory amendments involving 42 CFR §§ 493.1291(f) and 493.2 to solve these CLIA issues. The intent of these proposed amendments is solely to expand the list of permissible recipients of lab results, not to expand the purposes for which those results may be disclosed. Therefore, these amendments would not permit a disclosure which the HIPAA Privacy Regulations would prohibit (in the absence of state law restricting the list of permissible recipients of test results), and it would not permit the disclosure of a test result where state law prohibits disclosure of test results of that type due to their sensitive nature (*e.g.*, HIV results). Instead, the proposed amendments are aimed at scenarios in which the disclosure would be permitted by HIPAA but would be prohibited by state law merely because the intended recipient is not defined as an "authorized person" for receipt of lab results from a laboratory. The alternatives are listed below in order of preference.

CLIA Amendment Alternative 1: Revision of 42 CFR § 493.1291(f)

Test results must be released to the authorized person who ordered the test. In addition, notwithstanding any contrary State law defining who is an individual authorized to order tests or receive test results or both, test results may be released to:

(1) The laboratory that initially requested the test, if applicable;
(2) Any person designated to receive the test results by the authorized person who ordered the test;
(3) A "covered entity", as defined in 45 C.F.R. § 160.103; and
(4) A "business associate" of a covered entity, as defined in 45 C.F.R. § 160.103.

This section shall not be construed to permit the disclosure of any specific type of test result to any of the persons or entities named herein where the disclosure of test results of that type is otherwise prohibited by State or Federal law.

Rationale for CLIA Amendment Alternative 1
The first alternative is to revise 42 CFR § 493.1291(f), which currently provides that test results must be released only to authorized persons, and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test. The proposed revision would require that test results must be released to the authorized person who ordered the test, but would provide that in addition, notwithstanding contrary state law, test results may be released to certain other listed recipients. These recipients would include a referring laboratory; anyone designated by the authorized person who ordered the test; and a "covered entity" or a "business associate" as defined in the HIPAA Privacy Regulations. This alternative eliminates any reference to the undefined term "individual responsible for using the test results"; makes a distinction between mandatory and permissive test result disclosure; and responsibly expands the group of permissible recipients of test results by ensuring that those who receive the results are either closely associated with the patient's care or are governed by HIPAA-related safeguards. This alternative would permit states to define those to whom results must be disclosed, but would prohibit states from disallowing result delivery to the additional persons named in this section.

CLIA Amendment Alternative 2: Addition to 42 CFR § 493.2
Authorized person means an individual authorized under State law to order tests or receive test results or both. In addition, notwithstanding any contrary State law defining who is an individual authorized to order tests or receive test results or both, authorized person means:

(a) Any person designated to receive the test results by the authorized person who ordered the test;
(b) A "covered entity", as defined in 45 C.F.R. § 160.103; and
(c) A "business associate" of a covered entity, as defined in 45 C.F.R. § 160.103.

This definition shall not be construed to permit the disclosure of any specific type of test result to any of the persons or entities named herein where the disclosure of test results of that type is otherwise prohibited by State or Federal law.

Rationale for CLIA Amendment Alternative 2
The second alternative is to revise the definition of "authorized person" by amending 42 CFR § 493.2 to add that in addition to an individual authorized under State law to order tests, receive tests, or both, it includes a referring lab, any person designated by the authorized person who ordered the test, and any covered entity or business associate, notwithstanding any state law to the contrary. Like the third alternative, this definition would further clarify the meaning of 42 CFR § 493.1291(f), and would responsibly expand the group of permissible recipients of test results by ensuring that those who receive the results are either closely associated with the patient's care or are governed by HIPAA-related safeguards. This alternative would also continue to permit states to define "authorized persons", but would prohibit states from disallowing result delivery to the persons expressly included in the new definition.

CLIA Amendment Alternative 3: Addition to 42 CFR § 493.2
Individual responsible for using the test results means, notwithstanding any contrary State law defining who is an individual authorized to order tests or receive test results or both:

(a) Any person designated to receive the test results by the authorized person who ordered the test;
(b) A "covered entity", as defined in 45 C.F.R. § 160.103; and
(c) A "business associate" of a covered entity, as defined in 45 C.F.R. § 160.103.

This definition shall not be construed to permit the disclosure of any specific type of test result to any of the persons or entities named herein where the disclosure of test results of that type is otherwise prohibited by State or Federal law.

Rationale for CLIA Amendment Alternative 3

The third alternative is to define the term "individual responsible for using the test results", which appears in 42 CFR § 493.1291(f) but is currently undefined, by adding its definition in 42 CFR § 493.2. As proposed, the term would include any person designated by the authorized person who ordered the test and any covered entity or business associate, notwithstanding any state law to the contrary. This definition would further clarify the meaning of 42 CFR § 493.1291(f), and would responsibly expand the group of permissible recipients of test results by ensuring that those who receive the results are either closely associated with the patient's care or are governed by HIPAA-related safeguards. This alternative would also continue to permit states to define "authorized persons", but would prohibit states from disallowing result delivery to the persons expressly included in the new definition.

HIE barrier(s) addressed:
BR_1. Range within organizations of misinterpretation and/or application of laws or regulation
BR_3. Lack of policy standardization across entities
BR_5. Lack of interoperability between processes and technology
BR_7. Conflicting or outdated federal or state laws or regulations.

HIE type: 1. Direct Patient Care, 2. Payer, 3. Secondary Use, 4. State Government / Public Health

HIE type (Groups 1 – 4): 1. Direct Patient Care; 2. Payer; 4. State Government / Public Health

HIE model affected (E2E, PO HIE): 1. E2E – Entity to Entity; 2. PO HIE – Person Oriented Health Information Exchange

Applicability of solution: CMS, North Carolina General Assembly

Stakeholders affected (1 – 18):
1. Clinicians
2. Physician Groups
3. Federal Health Facilities
4. Hospitals
5. Payers
7. Community clinics and health centers
8. Laboratories
10. Long term care facilities and nursing homes
12. Corrections facilities
13. Professional associations and societies
14. Medical; public health schools; research
15. Quality improvement organizations
16. Consumers or consumer organizations
17. State government
18. Other RHIO, NHIN, American Clinical Laboratory Association, ONC

Privacy & security domain (s) addressed (1 – 9):

Domains	
1. Authentication	
2. Authorization	X
3. Identity Matching	
4. Transmission	
5. Integrity	
6. Event Audit	
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues: Perception of increased risks to privacy. Determine scope of "secondary uses of information."

HIPAA and North Carolina Law

NCGS § 8 – 53
Communications between physician and patient
This North Carolina statute resides in the evidentiary section of the General Statutes, but it has been interpreted to prohibit uses and disclosures of patient information in other contexts absent the patient's authorization or a court order. This statute has emerged as the most often-cited barrier to exchange of health information in the State.

Solution: Prepare or revise statutes to minimize perceived conflicts between NCGS § 8 – 53 and HIPAA with respect to sharing health information for treatment, payment, and operations and other uses or disclosures for which patient authorization is not required under HIPAA.

Rationale for Solution: Because this statute is generally determined to require patient consent prior to releasing health information for treatment, payment, and health care operations, such a revision to the statutory scheme should clarify that such releases without consent are acceptable and should reduce the delay in exchanging health information for these important purposes,

HIE barrier(s) addressed: BR_1. Range within organizations of misinterpretation and/or application of laws or regulation; BR_2. Lack of business incentives to exchange information; BR_3. Lack of policy standardization across entities; BR_4. Lack of security standardization across entities; BR_5. Lack of interoperability between processes and technology; BR_7. Conflicting or outdated federal or state laws or regulations

HIE type (Groups 1 – 4): 1. Direct Patient Care; 2. Payer; 3. Secondary Use: Operations, Marketing, Research, Law Enforcement; 4. State Government / Public Health

HIE model affected (E2E, PO HIE): 1. E2E – Entity to Entity; 2. PO HIE – Person Oriented Health Information Exchange

Applicability of solution: State of North Carolina General Assembly, All covered entities under HIPAA and other stakeholders

Stakeholders affected (1 – 18): ALL

Privacy & security domain (s) addressed (1 – 9):

Domains	
1. Authentication	
2. Authorization	
3. Identity Matching	
4. Transmission	
5. Integrity	
6. Event Audit	
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues:

Opposition to specific changes is possible. Need to assess potential unintended consequences of a broad amendment. For those who interpret NCGS § 8 – 53 to be a barrier to uses and disclosures of health information, the extent of this barrier is pervasive.

Technology Solutions

Adopt Security Standards

As the health care industry moves toward the realization of the Nationwide Health Information Network, HIPAA Privacy and Security becomes not only a compliance issue, but a sound business practice. The HIPAA Security Rule, 45 CFR §§ 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule, required by covered entities engaged in the exchange of certain electronic transactions, attempts to ensure the availability, confidentiality and integrity of "protected health information." While many health care organizations within North Carolina supported the HIPAA reforms as early adopters, its lack of standards and enforcement continue to present areas of ambiguity and complexity among our stakeholders. Our proposed solutions seek to address areas of ambiguity and complexity indicated by the following examples.

Page 8335 of the Rule states, "In this final rule, we replace the term 'requirement' with 'standard.'" Page 8336 of the Rule states, "In this final rule, we adopt both 'required' and 'addressable' implementation specifications. We introduce the concept of 'addressable implementation specifications' to provide covered entities additional flexibility with respect to compliance with the security standards. In meeting standards that contain addressable implementation specifications, a covered entity will ultimately do one of the following: (a) Implement one or more of the addressable implementation specifications; (b) implement one or more alternative security measures; (c) implement a combination of both; or (d) not implement either an addressable implementation specification or an alternative security measure."

According to the International Information Systems Security Certification Consortium (ISC)², standards are "mandatory activities, actions, rules, or regulations designed to provide policies with the support structure and specific direction they require to be meaningful and effective. It is a specific product or mechanism that is selected for universal use throughout the organization in order to support the policy." The intent of the Rule's flexibility and scalability of the implementation specifications tends to make measuring its effectiveness or compliance to the Rule a subjective exercise.

The processes of Authentication and Authorization for persons seeking access to electronic health information have often been administered separately, leading to opportunities for inconsistencies in user accounts and actual data access. In our proposed solutions, we consider both processes integral to standard access control management.

In order for individuals to authorize the electronic exchange of their health information, they must have confidence that the system is developed to prevent access to their information unless they have consented to it. Also, health care entities must be able to trust that the information originated from an authorized sender (authentication) and that it has not been modified while it was being transmitted (encryption).

Another important characteristic of authenticating the validity of a person's identity is a process called "identity matching." This is an important process for individual providers who deal with information about a specific patient that comes from more than one entity, where the individual entities may have different identification criteria. This process takes place when a user conducts a search such as those on Google or Yahoo. The user enters the information he or she is looking for and the search engine replies back with multiple choices that match the information entered. The user then clicks on the link to determine if that is what he or she is looking for.

The North Carolina Office of Information Technology Services developed and are carefully implementing the Identity Management Service (NCID -- see https://www.ncid.its.state.nc.us/) for the purpose of

authenticating users who subscribe to the state's online services. The state of Florida's Agency of Healthcare Administration established a record locator service similar to a hospital's e-Master Patient Index. Florida's record locator service works as an identity matching engine and manages access to the information about specific individuals.

By leveraging the infrastructure currently in place and partnering with other states like Florida as itbuilds the Florida Health Information Network, North Carolina could launch the building of an information security framework needed to participate in an interoperable health information exchange (HIE) that is consumer-centric, as described in the President's vision.

The industry-wide adoption of information security standards regarding authentication and authorization would be critical to building user trust and ensuring the confidentiality, availability, and integrity of the information.

Solution(s):
We are proposing the adoption of Health Information Exchange (HIE) security standards in the area of authentication and access authorization of the individual, and encryption to safeguard the information while in transit.

Amend the HIPAA Security Rule
45 CFR §§ 164.308, 164.310, and §164.312(e)(1)
Amend the "addressable" implementation specifications to "required."
Amend the term ''requirement'' with ''standard.
Require encryption during the transmission of information.

Rationale for Solution(s):

The intent of the HIE security standards is designed to support the HIPAA Privacy Regulations as required in 45 CFR §164.530 c. These standards will provide specific design requirements and implementation direction to the NHIN service providers and participants as well as approximately 28 - 45% of covered entities who still seek to comply with the regulations (US Healthcare Industry HIPAA Compliance Survey Results, Winter 2006, HIMSS and Phoenix Health Systems).

The process by which standards are designed and adopted would first engage the policy makers, subject matter, and technical experts to consider the various standards currently implemented. The experts would also have the opportunity to collaborate as they explore the dependencies between the business processes and their technical components. The goal would be to adopt a set of security standards that would safeguard the information as it is transmitted.

Adopting a universally accepted information security standard such as the National Institute of Standards and Technology (NIST SP 800-53-1, *Revision 1: Recommended Security Controls for Federal Information Systems*, December, 2006) or ISO / IEC 27001 for Administrative, Physical and Technical Safeguards would address the complexity and ambiguity surrounding the safeguarding of health information as well as the misinterpretation of laws or regulations within HIPAA Privacy and Security.

Proposed North Carolina General Statute Health Data Exchange Act
In the event that the amendment of HIPAA is unfeasible, we propose an alternative solution to ensure that entities engaged in the exchange of electronic health information in North Carolina implement certain required information safeguards.

We propose the introduction a new North Carolina General Statute Health Data Exchange Act that would serve to clarify authorization requirements and inconsistencies. Possible authorization requirements can include:

- Characterizations and delimitations of the actual health care records and information and/or subsets that will be made available for exchange

Characterizations and delimitations of the actual health care records and information and/or subsets that will be made available for exchange

- Restriction categories (if necessary)
- 'Original' vs. 'copy'
- De-identified records
- Research-appropriate subsets (ad-hoc, based on research protocols)
- Local record (entity-specific) vs. complete PHI
- Time limitations (*e.g.*, regulatory requirements allowing destruction/disposal)

Clear identification of the participants and their roles and responsibilities with PHI exchange

- Provider entity and representatives
- Provider and alternates (staff, assistants, referrals, etc.)
- Patient
- Person-agent (*e.g.*, parent, guardian, spouse, etc.)
- Entity-agency and representatives
- Government/law enforcement agents/agencies
- Responsibilities, *e.g.*, protection; ownership; ability to consent, delegate, exchange, or destroy

Clearly defined processes, rules, and use cases that enable appropriate access to and exchange of PHI

- PHI lifecycle access restrictions
- Protection at rest, in use, and during exchange
- Treatment, payment and operation practices and processes
- Create, update, modify, view, disseminate, consent, delegate, delete/destroy
- Violation consequences

HIE barrier(s) addressed: BR_1. Range within organizations of misinterpretation and/or application of laws or regulation; BR_3. Lack of policy standardization across entities; BR_4. Lack of security standardization across entities; BR_5. Lack of interoperability between processes and technology; BR_7. Conflicting or outdated federal or state laws or regulations; BR_8a. Lack consumer input into the design of policy and technology; BR_8b. Lack of definition of consumer empowerment and methodology to its inclusion in policy and systems design

HIE type: 1. Direct Patient Care; 2. Payer; 3. Secondary Use: Operations, Marketing, Research, Law Enforcement; 4. State Government / Public Health

HIE model affected: 1. E2E – Entity to Entity; 2. PO HIE – Person-Oriented Health Information Exchange

Applicability of solution: HIE, RHIO, HIPAA covered entities and other parties exchanging electronic health information

Stakeholders affected (1 – 18): All

Privacy & security domain (s) addressed (1 – 9:

Domains	
1. Authentication	X
2. Authorization	X
3. Identity Matching	X
4. Transmission	X
5. Integrity	X
6. Event Audit	X
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues: Lack of consensus over implementation standards.

Consumer Empowerment Solutions

The United States health care industry is currently experiencing a technological transformation. Due to recent technological advances, information can be shared among many health care providers, with the goal being reduced medical errors and increased quality of care. With U.S. legislative mandates and calls for the adoption of a Nationwide Health Information Network (NHIN), RHIOs (Regional Health Information Organizations), EHRs (Electronic Health Records), and PHRs (Personal Health Records), the awareness of patient empowerment is emerging. A survey by the California HealthCare Foundation (Broder, 2006) found that most consumers want to have control over who accesses their medical information and that only three percent used an online medical record service. Janlori Goldman, privacy advocate and member of the Health Privacy Project (1999) calls for a "reversal of the technological status quo by demanding that technology be designed to empower individuals" by shifting the balance of power between "the individual and those seeking personal information," for example, through giving control of medical information to the patients. "Since this [PHR] approach empowers individuals to control all access to their own health information, it gives each consumer the freedom to establish their own personalized privacy policy" (Enrado, 2006) and decide how it will be shared across organizations such asRHIOs and the NHIN, both of which enable the infrastructure for sharing patient information across organizations such as hospitals and provider offices.

The sharing of medical information extends to external entities who utilize medical information for patient care purposes. Secondary users of health care data includeresearchers, marketing departments and businesses, public health organizations, insurance payers, and accreditation companies. There are also health record banks which allow patients to decide who has access to their medical records which are stored in a secure repository, similar to a financial bank (Enrado, 2006). However, these banks are interested in the ability to collect and sell patient information to external parties for research or marketing purposes (AMIA, 2006; Anonymous, June 28, 2006) "The lack of coherent policies and practices for the secondary use of health data presents a significant impediment to the goal of strengthening the US healthcare system" (AMIA, 2006). Ultimately, patients' trust in the security and privacy of their medical data will affect how they share their information, and, currently what is not clear is patients' awareness of the "trade-offs between legitimate concerns about their privacy and the benefits of making more complete information available to the providers" so that they can provide optimal care based on more comprehensive information (Tang and Lansky, 2005). The patient is the person with the most at stake and is in the best position to provide information to providers (Markle, 2006). Empowering a patient with the knowledge and ability to determine how his or hermedical information is shared will be critical in the emerging technological environment.

Traditionally, records in the health care industry have been paper-based, enabling strict accessibility to records. Due to advances in technology, managing the large amount of information involved in patient care has become much more important. Therefore, information has become the "key organizational currency" for which companies need to manage and control to "harness the power of the politic"' which comes from such control (Davenport, et al, 1992). There is no U.S. law to state who actually owns the patient medical record. Because the control of either the paper-based medical record or electronic medical record is in the provider's hands, traditionally, the question has been that of patient access to the record rather than ownership. There are concerns which have risen to question how access to personal health information (PHI) will be granted. Currently, the patient gives a "blanket statement" for a single entity, but patients may not understand these statements or want to give such generic access across health care entities. Technology must be in place so that PHI is not shared electronically when the patient opts out of sharing information with specific entities. Technology such as the PHR gives a feeling of empowerment to the patient for control of his or herinformation as well as increased participation in the health care process. Literature supports the definition of empowerment as self-determination over one's own life (Geller et al, 1998) as a result of having access to information and resources to enable an

informed choice (Wowra et al, 1999). Empowerment holds multiple interpretations for the marketplace and business, the community, the public sector, and the political system (Osborne, 1994), and over time, these interpretations have changed (Wilkinson, 1997). For e-healthcare, this involves analyzing patient access and control of medical information for self-determination of who the information will be shared with and for what purpose. This also inherently entails education of stakeholders as to the responsibilities involved with patient empowerment and the impact of technology on patients.

Develop Consumer Programs

NCHICA has formed a new council to engage patients (health care consumers) in providing input and feedback on topics related to health information. The North Carolina Consumer Advisory Council on Health Information NC CACHI is a unique health care consumer group formed for grassroots input and participation to explore ideas and issues surrounding health information and will provide an opportunity to influence both state and national policy with regard to health care consumers' ideas and concerns about health information and technology.

In order to achieve a diverse representation of North Carolina health care consumers, the individuals chosen to be the members of NC CACHI will have varied backgrounds including gender, age, race, education, geography, health status, recent experience with the health care system, etc. They will server rotating limited terms, attend monthly meetings and participate in that raise awareness on the effects of health information technology on the consumer. As part of the NC CACHI and NCHICA initiatives to gain consumer input, providers will also be interviewed during roundtable sessions to gain insight as to gaps and overlaps in the provider and consumer perspectives of health care information issues. Activities for council members include participation in consumer focus groups and research studies to find ways to educate and empower North Carolina health care consumers. NC CACHI will be assisted by a group of experts who will serve on a resource panel.

Initial calls for nominations of members were sent to organizations on the NCHICA membership roster. Currently there are seven council members, with interests represented in populations such as HIV/AIDS, the aging and elderly, and caregivers. There are six resource panel members who provide support in special topics such as PHRs, privacy, and security. The co-chairs of the council are responsible for administrative processes so that council members are able to focus on discussions of their concerns. The NC CACHI meetings have been held monthly since July, 2006. One initiative which is being developed by the council is to investigate the generation of PHRs for seniors, especially for use in crisis situations. Because of its leading initiatives, NC CACHI will serve as a role model for other states to create similar consumer advisory councils.

Rationale for Solution:

As the subject of the information to be exchanged and the intended users of personal health records, consumers generally do not have sufficient information to weigh the risks and benefits of health information technology and do not play an active role in the design and use of health information technology. Current health information software design methodology includes processes to identify the business problem automation will solve, plan the project, gather requirements, conduct security analyses, test the application, and implement software. They even include clinical experts on their design team to ensure usability and features to reflect standard clinical processes.

Effective in April of 2003, HIPAA required health care providers and health plans to develop policies and procedures that established the rights of individuals to access, copy, and amend their health information, request restrictions upon its use and disclosure, and file privacy complaints.

In August 2005 an Executive Order established the Office of the National Coordinator for Health Information Technology, whose mission is to provide leadership for the development and nationwide implementation of an interoperable health information technology infrastructure to improve the quality and efficiency of health care and the ability of consumers to manage their care and safety. The

same Executive Order established the American Health Information Community (AHIC), whose activities include coordination of the development of strategies and guidance to create electronic personal health management tools and to enhance informed consumer choice for health care.

As health information begins its transformation towards a consumer-controlled model, presumptions on the needs of the consumers without direct consumer participation could cause design errors that result in distrust and lack of adoption. Developing a program that seeks to define consumer empowerment, researches consumers' use of health information technology, raises awareness on the impacts of health information technology, and provides input on the usability of personal health records can engage consumers in the design and implementation of health care policies and technology.

Availing itself of the numerous AHIC documents regarding consumer empowerment, the HISPC project information, and personal experiences as health care consumers, the members of the council are unsure how AHIC intends to include consumers in the design of the NHIN or other health information technology initiatives. In North Carolina, medical professionals join associations such as the North Carolina Medical Society or the North Carolina Hospital Association to exchange ideas and participate in collaborative initiatives to improve their profession and the quality of health care. The legal and information security professionals also benefit from awareness and training programs within their associations. NC CACHI will seek to establish itselfas an independent body committed to representing the consumer's perspective on the changing landscape of health information technology.

HIE barrier addressed: BR_1. Range within organizations of misinterpretation and/or application of laws or regulation; BR_2. Lack of business incentives to exchange information; BR_3. Lack of policy standardization across entities; BR_4. Lack of security standardization across entities; BR_5. Lack of interoperability between processes and technology; BR_6. Lack of workable technology; BR_7. Conflicting or outdated federal or state laws or regulations; BR_8a. Lack consumer input into the design of policy and technology; BR_8b. Lack of definition of consumer empowerment and its applicability in systems methodology

HIE type (Groups 1 – 4): ALL

HIE model affected: 1. E2E – Entity to Entity, 2. PO HIE – Person-Oriented Health Information Exchange

Applicability of solution: Consumers, providers, and all health care stakeholders, especially consumers and providers

Stakeholders affected (1 – 18): ALL

Privacy & security domain (s) addressed (1 – 9):

Domains	
1. Authentication	X
2. Authorization	X
3. Identity Matching	X
4. Transmission	X
5. Integrity	X
6. Event Audit	X
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues:
Current laws regarding privacy and the "no call" registry may prohibit the Council from direct recruiting. The Council will develop strategies to overcome the distrust of technology among consumers and the perception that government is developing a NHIN "for" them. The Council will also develop strategies to encourage consumers to participate in the activities.

Explore Person-Oriented HIE

Establish a pilot project with adequate funding to explore the concept of the Person-Oriented Health Information Exchange (PO HIE).

Exploring PO HIEs
NC HISPC theorizes that a person-oriented health information exchange (PO HIE) has the potential for assuring high flow in a health information exchange while preserving privacy. It has a low potential to interfere with care to which the patient has consented and may speed appropriate care in cases where legal barriers to information release today are significant.

Background
Because consumer empowerment is among the top priorities for the development of an interoperable health information network, ONC established the Consumer Empowerment Workgroup within AHIC. The Workgroup will coordinate the development of strategies to create personal health management tools to enhance informed consumer choice for health care.

In an effort to support ONC's charge, the SWG and LWG evaluated how the scenarios and identified barriers would be affected if flow of the health information exchange originated from the person who was the subject of the information to the requesting entities rather than the traditional model of entity to entity exchange. As they researched background information on health care consumer empowerment, the SWG considered the consumer-oriented projects such as personal health records as described by the Markle Foundation's Connecting for Health, and person-centered RHIOs such as the Louisville Health Information Exchange (LOUHIE).

This important exercise taught the SWG that current policy and information systems are designed to facilitate health information exchange between entities. HIPAA requires the individual's right to access, copy, amend, and restrict his or herhealth information. NC General Statutes require an individual's authorization to release health information. There is uncertainty among the LWG as to how the PO HIE affects current laws and regulations. The Consumer Advisory Council is cautiously optimistic but has concerns about lack of consumer input into planning, design, and implementation of consumer-driven systems. The PO HIE has intrigued the SWG, and the workgroup anticipates further study into this model. The Steering Committee has recommended further exploration for North Carolina's health care policy makers, subject matter, and technical experts.

Rationale for Solution
In the last couple of years, considerations of the value of a health data exchange that puts the consumer/patient at the center of the exchange process have emerged in the form of private and public activities (*e.g.* products, conferences, whitepapers, and projects). The key idea in a Person-Oriented Health Information Exchange is that the provider of the data sends the data (along with a request to transmit the data) to a person-controlled software agent. The agent, as configured by the person who is the subject of the data, permits and completes appropriate exchanges and rejects others. This approach draws the patient into the health care process, eases the creation of personal health records and their associated applications, permits individual flexibility related to privacy, and returns the issue of who is included in the information flow related to a patient's care back to a dialogue between the patient and his/her health care provider(s).

The PO HIE, because it would reduce an entity's responsibility for controlling the elements of an exchange of health information, may provide a solution to some of the disparities among state and federal regulations. If the health care consumer, or her/his authorized delegate, is the gatekeeper to personal information, then each instance of exchange would be pre-authorized or made in a pre-defined manner. Potentially this may reduce the need for some regulatory changes. The process(es) for defining access authentication and delegation of authorization would need to be strict, as well as the overall audit function. The PO HIE could also work well with the "original" and "copy" concepts.

The pilot would have to address all data protection issues, contingencies for emergent circumstances whereby the health care consumer is unable to grant access to health care information, the possibility of access barriers for indirect providers such as laboratories, and the impact upon legitimate secondary uses and disclosures that are permissible under existing law.

Initiate the PO HIE concept for awareness purposes. Many health care consumers are unaware of the implications of access to personal health information and the consequences of unauthorized access and misuse of that information. Initiating a process that places the individual or delegate as the primary agent responsible for granting access would increase a sense of ownership and control to the consumers, and could provide an opportunity to educate individuals about privacy and security issues and responsibilities. The PO HIE concept could be the centerpiece in a comprehensive and consistent awareness strategy. Organizational and entity level awareness programs would serve to reinforce the information.

The PO HIE concept is one model that would address and has the potential to resolve a number of barriers identified in the Variations Report. Individual consumer involvement at the center of the health care information exchange may result in an enhanced awareness of privacy and security issues across the general population. The model would need to be supported by carefully defined policies for authentication, authorization (especially for personal delegates), protecting data in transit and at rest, and responsibilities of the individual for the care of this or her own records.

In a PO HIE, an intermediary agent/agency will make connections with health care providers. As such, a PO HIE could help to relieve concerns about direct access to provider networks by other providers. Each endpoint entity will have to be confident of the agent/agency connection. Technical solutions and policy definitions are necessary go ensure isolated access to authorized information.

HIE barrier addressed: BR_2. Lack of business incentives to exchange information; BR_3. Lack of policy standardization across entities; BR_4. Lack of security standardization across entities BR_5. Lack of interoperability between processes and technology; BR_7. Conflicting or outdated federal or state laws or regulations; BR_8a. Lack consumer input into the design of policy and technology; BR_8b. Lack of definition of consumer empowerment and its applicability in systems methodology

HIE type: 1. Direct Patient Care, 2. Payer, 3. Secondary Use: Operations, Marketing, Research, Law Enforcement, 4. State Government / Public Health

HIE model affected: 1. E2E – Entity to Entity, 2. PO HIE – Patient Centered Health Information Exchange

Applicability of solution: Persons who are subject of the health information exchange, entities

Stakeholders affected (1 – 18): All

Privacy & security domain (s) addressed (1 – 9):

Domains	
1. Authentication	X
2. Authorization	X
3. Identity Matching	X
4. Transmission	X
5. Integrity	X
6. Event Audit	X
7. Safeguards	X
8. Data classification	X
9. Policies	X

Potential barriers / issues:
One perception is that the PO HIE is a "new concept." The PO HIE approach has been adopted in the form of Personal Health Records for the employees of Dell, Walmart, and IBM. Kentucky has also done significant work in this area. Consumer participation is vital to the success of this concept. Therefore, awareness programs should be considered in the planning, design, and implementation of this concept.

The LWG has concerns that there could be a perception to policy makers that a PO HIE approach could be misconstrued as regulatory avoidance. Current exceptions to accessing the persons health information without authorization as stated in HIPAA and NC General Statutes would not change.

Conclusions and Next Steps

The HISPC project has convened a core group of North Carolina consumers and health care professionals from varying segments of the health care industry. The discussions within the VWG, LWG, SWG, Steering Committee, and Consumer Advisory Council meetings have generated interest in further exploring the barriers to exchange and implementing the solutions to those barriers. The Implementation Plan Report will propose high-level steps for interested stakeholders to consider as they plan for the implementation of the solutions.

The implementation challenge to the North Carolina stakeholders is that there is no executive-level mandate or sponsorship to actually implement the solutions at this time. Therefore, the next steps for the North Carolina stakeholders will be to:

5. Raise awareness on the benefits of health information technology adoption
6. Develop HIT thought leadership development programs
7. Engage the General Assembly into the process
8. Cultivate the Consumer Advisory Council

To participate in the continuing efforts or to view more information on the NC HISPC efforts please see the NCHICA site at: http://www.nchica.org/NCHISPC/intro.htm

Appendices

Business Practice Data

As instructed, the business practices data has been uploaded to AHRQ's HISPC portal.

Invitation to Participate in NC HISPC

What:	NC HISPC Work Session	**Date:**	10/1/06
Scenarios:	Group 1 Patient Care Scenarios 1-4, 6, and 8	**Time:**	12 – 4 pm
Type:	Patient Care	**Place:**	NCHICA Office

Congratulations! After reviewing your volunteer application, you have been confirmed to participate as an interviewee in the NC HISPC (Health Information Security and Privacy Collaborative) project.

Directions to the NCHICA office can be found at: http://www.nchica.org/AboutNCHICA/Location.htm

In preparation for your work session, we recommend that you read each of the attached scenarios. We also recommend that you bring appropriate materials such as policies, procedures, guidelines, standards, or periodicals to reference. We may ask for copies of public information such as statutes, standards, or regulations only. Proprietary information you choose to share will be used only to identify current practices and barriers related to those practices.

Upon arrival, all participants will register and sign a confidentiality agreement. These work sessions are designed to generate open discussions with your colleagues, therefore, all information shared during the work sessions are strictly confidential.

The discussions will center on describing your business practices related to exchanging individual health information with other entities as described in the scenario(s). For each scenario, we'll explore:

1. What is your current business practice if presented with this type of scenario?
2. Why is that your current business practice?
3. Does this business practice aid the exchange of health information with other entities?
4. Does this business practice present a barrier to exchanging health information?
5. Is this barrier appropriate to safeguard the information?
    a. Why is it appropriate?
    b. If not, could you recommend an alternate solution to removing this barrier?
6. How is this particular business practice affected in a manual or electronic environment?

Please confirm your attendance by accepting or declining this email invitation. After reading the scenarios and work session process, you may discover there are others in your organization who may contribute to this collaborative project. Feel free to invite them to participate by contacting our office.

Angie Santiago
NC HISPC Project Manager
919-558-9258 ext. 26
asantiago@nchica.org

NC HISPC Volunteer Request Application

First, Middle, Last Name:	
Title / Position:	
Organization Name:	
Organization Type: (refer to grid)	
Address:	
City, State, Zip Code:	
Email Address:	
Office Phone:	
Cell Phone:	
Contact Information:	
Current Project, Taskforce, Conference or Workgroup Name:	
Available Weekly Pro Bono Hours:	
Experience:	• IT Personnel; Project Management; Health care Implementations; Program Development, Public Policy; Systems Tools Development

Please send this completed survey to:
Angie Santiago
NC HISPC Project Manager
919-558-9258 x 26
asantiago@nchica.org

NC HISPC Volunteer Confirmation and Confidentiality Agreement

First, Middle, Last Name:	
Title / Position:	
Organization Name:	
Stakeholder Type: (*e.g.* hospital, physician, payer, vendor, etc.)	
Address:	
City, State, Zip Code:	
Email Address:	
Office Phone:	
Cell Phone:	
Current Project, Taskforce, Conference or Workgroup Name:	
Work Experience:	
Available Weekly Pro Bono Hours:	

CONFIDENTIALITY STATEMENT

As required by the Federal Contract and as a participant in the North Carolina Health Information Security and Privacy Collaboration Project sub-contracted to NCHICA, I hereby agree that I will not at any time disclose or use, either during or subsequent to my participation, any information, knowledge or data which I receive or develop during my tenure in the Project which is considered proprietary by NCHICA, RTI International, National Governor's Association, the Agency for Health Research and Quality, or the State of North Carolina which relates to the Project. Such information, knowledge, or data may include, but is not limited to: discussions, processes, assessments, status reports, print screens, presentations, contact lists, diagrams, draft or final documents, and accounting or financial data.

I further agree that upon termination of my tenure with the Project, I shall promptly return or destroy any and all documents containing the above information, knowledge or data, or relating thereto, to NCHICA.

_____

Name (Please print) Date:

_____

Signature

Please send or fax this form to:
Attn: Angie Santiago
NC HISPC Project Manager

Sub-Group 1 Scenario Analysis

Group A interactions:

1. Emergent transfer of information between two hospitals in different states

Group B interactions:

1. The elective referral of a patient from a facility (substance abuse treatment) to a primary care facility for evaluation and treatment of suspected medical problem

Group C interactions:

Interactions:

1. Non-emergent transfer of information from the hospital psychiatric unit to the skilled nursing facility
2. Non-emergent transfer of information by the physician to an outsourced transcription service (in a foreign country)
3. Viewing of patient health information on an outsourced transcription service (in a foreign country) on a web portal and providing an electronic signature
4. Non-emergent transfer of information by an outsourced transcription service (in a foreign country) and the physician
5. Non-emergent transfer of information by an agent of the physician to the skilled nursing facility

Group D interactions:

1. Non-emergent transfer of information between a hospital and an outpatient clinic in different states

= need for info

Group A Interaction requires:

1. Consent for request of information as defined by circumstances (release of information)
2. Determination of patient's ability to provide consent
    a. "Time of consent" circumstances that may change ability of individual to provide authorization (impairment secondary to new condition requiring ED visit)
    b. Chronic health impairment (dementia)
3. Communication of health record request from one institution to another
    a. Verification that appropriate party contacted (right institution, right individual to handle request)
    b. Verification of identity of requesting party
    c. Verification of valid patient consent by hospital holding records
    d. Determining pertinence of entire health record (*i.e.*Mental health information)
    e. Transmission of health record information from possessing institution to requesting institution
4. Verification of secure receipt of information (sending hospital)
5. Securing received health information (the releasing hospital (B) should be assured that the receiving hospital will secure the information adequately, before B can release it responsibly)

= method of gaining info (vs other source, like patient's copy of records, or local diagnosis)

Group B interaction requires:

1. Patient consent for referral for medical evaluation
2. Patient consent (release of information) for reque
3. Determination of patients ability to provide consent
4. Communication of health record request from one institution to another
    a. Verification that appropriate party contacted (right institution, right individual to handle request)
    b. Verification of identity of requesting party
    c. Verification of valid consent to transfer health information (including mental health/substance abuse data)

   d. Determining pertinence of entire health record
   e. Transmission of health record information from possessing institution to requesting institution
5. Verification of secure receipt of information (sending hospital)
6. Transmission of evaluation and treatment information back to referring facility/health care provider

Group C interaction requires:

1. Determination of patient's ability to provide consent
   a. Patient consent for referral to skilled nursing facility
   b. Patient consent for release of information (medical records) to skilled nursing facility
2. Transfer of patient from the hospital psychiatric unit to the skilled nursing facility
   a. Contact facility and notify of intention to transfer
   b. Determine willingness of institution to accept transfer (has capacity to accommodate patient) and accept responsibility of patient
   c. Communicate discharge documents
   d. Communication of request for complete health records from accepting institution to transferring institution
   e. Verification that appropriate party contacted (right institution, right individual to handle request)
   f. Verification of identity of requesting party
   g. Verification of valid consent to transfer health information (including mental health/substance abuse data)
   h. Determining pertinence of entire health record (if consent not clearly defined)
   i. Transmission of health record information from possessing institution to requesting institution
3. Verification of secure receipt of information (sending hospital)
4. Dr X evaluates patient
   a. Facility accepts Dr X's credentials, and provides physical access to the patient
   b. Facility gives Dr X access to the content of the patient's electronic health record (EHR), but does not allow direct update
   c. Dr X prepares his assessment using his practice's technical facilities (including the off-shoe dictation service)
   d. Dr X delivers the assessment through a secure means, for inclusion in the Facility's EHR

Group D interaction requires:

1. Consent for request of information as defined by circumstances. (release of information)
2. Communication of health record request from one institution to another.
   a. Verification that appropriate party contacted (right institution, right individual to handle request)
   b. Verification of identity of requesting party
   c. Verification of valid consent by hospital holding records
   d. Determining pertinence of entire health record (*i.e.* HIV status)
   e. Transmission of health record information from possessing institution to requesting institution
3. Verification of secure receipt of information (sending hospital)
4. Securing received health information

Mitigating factors:

1. Group A
   a. Law enforcement involvement of potential crime
   b. Patient impaired from three potential viewpoints:
      i. "Confused" either acutely (head injury) or
      ii. Medication induced (newly Rx medication in elderly) or
      iii. Mental health issue ("psychosis")
2. Group B
   a. Patient referred from substance abuse facility

   b. Any impairment issues?
   c. Substance abuse or related conditions (mental health issues
3. Group C
   a. Patient referred from substance abuse facility
   b. Any impairment issues?
   c. Substance abuse or related conditions (mental health issues)
   d. Dr. X : Physical access to facility
   e. Dr. X: Access to EHR (facility he has no privileges? Verification of credentials?)
   f. Dr.X: Dictation of health care note to transcription service in foreign country.
   g. Dr. X: Accesses note on server at transcription service, "electronic signature"
   h. Note downloaded by Dr. X employee and emailed (encrypted) to nursing home
   i. Nursing home can't decode note.
4. Group D
   a. Patient x is HIV positive
   b. Obtaining BrCa genetic test results of another individual
   c. The other individual is deceased

Group A barriers:

1. Knowledge of acceptable procedures (hospital, state and federal policies)
   a. Definitions of impairment
   b. Rules /laws regarding next of kin providing consent (living will?)
   c. Rules/laws for interstate transfer of health information
   d. Rules/laws for transfer of all health care information (*i.e.* Mental health information). Differ from transfer of "non-sensitive" data?
   e. Rules/laws for methods of transmission of health record information from possessing institution to requesting institution. (Electronic?)
   f. Rules/laws for verification of secure receipt of information (sending hospital)
   g. Verification of identities
   h. Rules /laws regarding institutional responsibilities towards transfer of information to law enforcement
2. Secure verifiable technology for acquisition and transmission of protected health information in a sufficiently timely manner (registered US Mail is secure and verifiable, but is not fast enough)

Group B barriers:

1. Knowledge of acceptable procedures (hospital, state and federal policies), or previously established methods
   a. Rules/laws for transfer of all health care information (*i.e.*substance abuse and/or mental health information). Differ from transfer of "non-sensitive" data?
   b. Rules/laws for methods of transmission of health information (HI) from possessing institution to requesting institution (Electronic?)
   c. Verification of identities
   d. Rules/laws for verification of secure receipt of information (sending hospital)

2. Secure verifiable technology for acquisition and transmission of protected health information

Group C barriers:

1. Knowledge of acceptable procedures (hospital, state and federal policies)
   a. Rules /laws regarding providing consent (release of information)
   b. Rules/laws for transfer of all health care information (*i.e.*substance abuse and/or mental health information). Does the transfer of mental health information differ from transfer of "non-sensitive" data? (yes)
   c. Rules/laws for methods of transmission of health record information from possessing institution to requesting institution (Electronic?)
   d. Verification of identities
   e. Rules/laws for verification of secure receipt of information (sending hospital)
   f. Rules /laws regarding outsourcing of dictation transcription to third party company in a foreign country

g. Rules /laws and security issues regarding use of portal website for posting of health information
h. Rules /laws regarding electronic signature
i. Standards for encryption and transmission of health information

2. Secure verifiable technology for acquisition and transmission of protected health information
    a. The technical means exist in this case, but are not sufficiently coordinated (Doctor did not give facility his decryption key, and they were not equipped to look it up elsewhere)

Group D Barriers:

1. Knowledge of acceptable procedures (hospital, state and federal policies)
    a. Rules /laws regarding providing consent (release of information)
    b. Rules/laws for transfer of all health care information (*i.e.*HIV results). Does the elective transfer of HIV status health information differ from transfer of “non-sensitive” data? (yes)
    c. Does the elective transfer of genetic health information differ from transfer of “non-sensitive” data?
    d. Rules/laws for methods of transmission of health record information from possessing institution to requesting institution (Electronic?)
    e. Verification of identities
    f. Rules/laws for verification of secure receipt of information (sending hospital)

Related NC Legal Drivers

NCGS § 90-21.13(a). Informed Consent.
If patient is not capable, NCGS § 90-21.13(a) allows for consent by the patient's spouse, parent, guardian, nearest relative, or other person authorized to give consent. Also may be able to bypass consent pursuant to the emergency exception (NCGS § 90-21.13(a)(3)), which applies when delay necessary to obtain consent would be dangerous to the patient and the emergency is such that "a reasonable person, under all the circumstances, would have undergone such treatment had he been advised by the healthcare provider."

NCGS § 8-53. Communications between physician and patient.
"No person, duly authorized to practice physic or surgery, shall be required to disclose any information which he may have acquired in attending a patient in a professional character, and which information was necessary to enable him to prescribe for such patient as a physician, or to do any act for him as a surgeon, and no such information shall be considered public records under G.S. 132-1. Confidential information obtained in medical records shall be furnished only on the authorization of the patient, or if deceased, the executor, administrator, or, in the case of unadministered estates, the next of kin. Any resident or presiding judge in the district, either at the trial or prior thereto, or the Industrial Commission pursuant to law may, subject to G.S. 8-53.6, compel disclosure if in his opinion disclosure is necessary to a proper administration of justice. If the case is in district court the judge shall be a district court judge, and if the case is in superior court the judge shall be a superior court judge." (1885, c. 159; Rev., s. 1621; C.S., s. 1798; 1969, c. 914; 1977, c. 1118; 1983, c. 410, ss. 1, 2; c. 471.)"

NCGS § 122C-55(d) and (e): Mental Health Information:
Pursuant to NCGS 122C-55(d) and (e), a mental healthcare provider may release mental health information about patient (i) where there is an imminent danger to the patient's health or safety, or (ii) to a physician providing emergency services to the patient.

NCGS § 130A-148. HIV confidentiality – "A test for AIDS virus infection may also be performed upon any person solely by order of a physician licensed to practice medicine in North Carolina who is rendering medical services to that person when, in the reasonable medical judgment of the physician, the test is necessary for the appropriate treatment of the person; however, the person shall be informed that a test for AIDS virus infection is to be conducted, and shall be given clear opportunity to refuse to submit to the test prior to it being conducted, and further if informed consent is not obtained, the test may not be performed. A physician may order a test for AIDS virus infection without the informed consent of the person tested if the person is incapable of providing or incompetent to provide such consent, others authorized to give consent for the person are not available, and testing is necessary for appropriate diagnosis or care of the person."

NCGS § 58-3-215. Genetic Information and Health Insurance – "For the purpose of this report, routine physical measurements, blood chemistries, blood counts, urine analyses, tests for abuse of drugs, and tests for the presence of human immunodeficiency virus are not to be considered genetic tests. . . .

(c) No insurer shall:

(1) Raise the premium or contribution rates paid by a group for a group health benefit plan on the basis of genetic information obtained about an individual member of the group.

(2) Refuse to issue or deliver a health benefit plan because of genetic information obtained about any person to be insured by the health benefit plan.

(3) Charge a higher premium rate or charge for a health benefit plan because of genetic information obtained about any person to be insured by the health benefit plan."

NCGS § 95-28.1A. Discrimination against persons based on genetic testing or genetic information prohibited.
“(a) No person, firm, corporation, unincorporated association, State agency, unit of local government, or any public or private entity shall deny or refuse employment to any person or discharge any person from employment on account of the person's having requested genetic testing or counseling services, or on the basis of genetic information obtained concerning the person or a member of the person's family. This section shall not be construed to prevent the person from being discharged for cause.

(b) As used in this section, the term "genetic test" means a test for determining the presence or absence of genetic characteristics in an individual or a member of the individual's family in order to diagnose a genetic condition or characteristic or ascertain susceptibility to a genetic condition. The term "genetic characteristic" means any scientifically or medically identifiable genes or chromosomes, or alterations or products thereof, which are known individually or in combination with other characteristics to be a cause of a disease or disorder, or determined to be associated with a statistically increased risk of development of a disease or disorder, and which are asymptomatic of any disease or disorder. The term "genetic information" means information about genes, gene products, or inherited characteristics that may derive from an individual or a family member.”

NCGS § 90-401. Referral fees and payment for certain solicitations prohibited.
“A healthcare provider shall not financially compensate in any manner a person, firm, or corporation for recommending or securing the healthcare provider's employment by a patient, or as a reward for having made a recommendation resulting in the healthcare provider's employment by a patient. No healthcare provider who refers a patient of that healthcare provider to another healthcare provider shall receive financial or other compensation from the healthcare provider receiving the referral as a payment solely or primarily for the referral. This section shall not be construed to prohibit a healthcare provider's purchase of advertising which does not entail direct personal contact or telephone contact of a potential patient.”

NCGS § 130A -131.8 Report of blood levels in children – “All laboratories doing business in this State shall report to the Department all blood lead test results for children less than six years of age and for individuals whose ages are unknown at the time of testing. Reports shall be made within five working days after test completion on forms provided by the Department or on self-generated forms containing: the child's full name, date of birth, sex, race, address, and Medicaid number, if any; the name, address, and telephone number of the requesting healthcare provider; the name, address, and telephone number of the testing laboratory; the laboratory results, the specimen type — venous or capillary; the laboratory sample number, and the dates the sample was collected and analyzed. The reports may be made by electronic submissions.”

NCGS § 130A – 131.17 Confidentiality of Information; Research – “(a) All information collected and analyzed by the Program pursuant to this Part shall be confidential insofar as the identity of the individual patient is concerned. This information shall not be considered public record open to inspection. Access to the information shall be limited to Program staff authorized by the Director of the State Center for Health and Environmental Statistics. The Director of the State Center for Health and Environmental Statistics may also authorize access to this information to persons engaged in demographic, epidemiological, or other similar scientific studies related to health. The Commission shall adopt rules that establish strict criteria for the use of monitoring Program information for scientific research. All persons given authorized access to Program information shall agree, in writing, to maintain confidentiality.

(b) All scientific research proposed to be conducted by persons other than authorized Program staff using the information from the Program, shall first be reviewed and approved by the Director of the State Center for Health and Environmental Statistics and an appropriate committee for the protection of human subjects which is approved by the United States Department of Health and Human Services pursuant to Part 46 of Title 45 of the Code of Federal Regulations. Satisfaction of the terms of the Commission's rules for data access shall entitle the researcher to obtain information from the Program and, if part of the research protocol, to contact case subjects.

(c) Whenever authorized Program staff propose a research protocol that includes contacting case subjects, the Director of the State Center for Health and Environmental Statistics shall submit a protocol describing the research to the State Health Director and to an appropriate committee for the protection of human subjects which is approved by the United States Department of Health and Human Services pursuant to Part 46 of Title 45 of the Code of Federal Regulations. If and when the protocol is approved by the committee and by the State Health Director pursuant to the rules of the Commission, then Program staff shall be entitled to complete the approved project and to contact case subjects.

(d) The Program shall maintain a record of all persons who are given access to the information in the system. The record shall include the following:

(1) The name of the person authorizing access;

(2) The name, title, and organizational affiliation of persons given access;

(3) The dates of access; and

(4) The specific purposes for which information is to be used.

The record required under this subsection shall be open to public inspection during normal operating hours.

(e) Nothing in this section prohibits the Program from publishing statistical compilations relating to birth defects that do not in any way identify individual patients."

NCGS § 130A – 152 Immunization Required – "(a) Every child present in this State shall be immunized against diphtheria, tetanus, whooping cough, poliomyelitis, red measles (rubeola) and rubella. In addition, every child present in this State shall be immunized against any other disease upon a determination by the Commission that the immunization is in the interest of the public health. Every parent, guardian, person in loco parentis and person or agency, whether governmental or private, with legal custody of a child shall have the responsibility to ensure that the child has received the required immunization at the age required by the Commission. If a child has not received the required immunizations by the specified age, the responsible person shall obtain the required immunization for the child as soon as possible after the lack of the required immunization is
determined.

(b) Repealed by Session Laws 2002-179, s. 10, effective October 1, 2002.

(c) The Commission shall adopt and the Department shall enforce rules concerning the implementation of the immunization program. The rules shall provide for:

(1) The child's age at administration of each vaccine;

(2) The number of doses of each vaccine;

(3) Exemptions from the immunization requirements where medical practice suggests that immunization would not be in the best health interests of a specific category of children;

(4) The procedures and practices for administering the vaccine; and

(5) Redistribution of vaccines provided to local health departments.

(c1) The Commission for Health Services shall, pursuant to G.S. 130A-152
and G.S. 130A-433, adopt rules establishing reasonable fees for the administration of vaccines and rules limiting the requirements that can be placed on children, their parents, guardians, or custodians as a

condition for receiving vaccines provided by the State. These rules shall become effective January 1, 1994.

(d) Only vaccine preparations which meet the standards of the United States Food and Drug Administration or its successor in licensing vaccines and are approved for use by the Commission may be used.

(e) When the Commission requires immunization against a disease not listed in paragraph (a) of this section, or requires an additional dose of a vaccine, the Commission is authorized to exempt from the new requirement children who are or who have been enrolled in school (K-12) on or before the effective date of the new requirement."

NCGS § 130A – 153 Obtaining immunization; reporting by local health departments; access to immunization information in patient records; immunization of minors – "(a) The required immunization may be obtained from a physician licensed to practice medicine or from a local health department. Local health departments shall administer required and State-supplied immunizations at no cost to the patient. The Department shall provide the vaccines for use by the local health departments. A local health department may redistribute these vaccines only in accordance with the rules of the Commission.

(b) Local health departments shall file monthly immunization reports with the Department. The report shall be filed on forms prepared by the Department and shall state, at a minimum, each patient's age and the number of doses of each type of vaccine administered.

(c) Immunization certificates and information concerning immunizations contained in medical or other records shall, upon request, be shared with the Department, local health departments, and the patient's attending physician. In addition, an insurance institution, agent, or insurance support organization, as those terms are defined in G.S. 58-39-15, may share immunization information with the Department. The Commission may, for the purpose of assisting the Department in enforcing this Part, provide by rule that other persons may have access to immunization information, in whole or in part.

(d) A physician or local health department may immunize a minor with the consent of a parent, guardian, or person standing in loco parentis to the minor. A physician or local health department may also immunize a minor who is presented for immunization by an adult who signs a statement that he or she is authorized by a parent, guardian, or person standing in loco parentis to the minor to obtain the immunization for the minor."

NCGS § 130A-155 Submission of certificate to child care facility, preschool and school authorities; record maintenance; reporting **– "**(a) No child shall attend a school (pre K-12), whether public, private or religious, a child care facility as defined in G.S. 110-86(3), unless a certificate of immunization indicating that the child has received the immunizations required by G.S. 130A-152 is presented to the school or facility. The parent, guardian, or responsible person must present a certificate of immunization on the child's first day of attendance to the principal of the school or operator of the facility, as defined in G.S. 110-86(7). If a certificate of immunization is not presented on the first day, the principal or operator shall present a notice of deficiency to the parent, guardian or responsible person. The parent, guardian or responsible person shall have 30 calendar days from the first day of attendance to obtain the required immunization for the child. If the administration of vaccine in a series of doses given at medically approved intervals requires a period in excess of 30 calendar days, additional days upon certification by a physician may be allowed to obtain the required immunization. Upon termination of 30 calendar days or the extended period, the principal or operator shall not permit the child to attend the school or facility unless the required immunization has been obtained.

(b) The school or child care facility shall maintain on file immunization records for all children attending the school or facility which contain the information required for a certificate of immunization as specified in G.S. 130A-154. These certificates shall be open to inspection by the Department and the local health department during normal business hours. When a child transfers to another school or facility, the school

or facility which the child previously attended shall, upon request, send a copy of the child's immunization record at no charge to the school or facility to which the child has transferred.

(c) Within 60 calendar days after the commencement of a new school year, the school shall file an immunization report with the Department. The child care facility shall file an immunization report annually with the Department. The report shall be filed on forms prepared by the Department and shall state the number of children attending the school or facility, the number of children who had not obtained the required immunization within 30 days of their first attendance, the number of children who received a medical exemption and the number of children who received a religious exemption.

(d) Any adult who attends school (pre K-12), whether public, private or religious, shall obtain the immunizations required in G.S. 130A-152 and shall present to the school a certificate in accordance with this section. The physician or local health department administering a required vaccine to the adult shall give a certificate of immunization to the person. The certificate shall state the person's name, address, date of birth and sex; the number of doses of the vaccine given; the date the doses were given; the name and addresses of the physician or local health department administering the required immunization; and other relevant information required by the Commission."

NCGS § 130A – 441 Reporting – "(a) Health assessment results shall be submitted to the school principal by the medical provider on health assessment transmittal forms developed by the Department and the Department of Public Instruction.

(b) Each school having a kindergarten shall maintain on file the health assessment results. The files shall be open to inspection by the Department, the Department of Public Instruction, or their authorized representatives and persons inspecting the files shall maintain the confidentiality of the files. Upon transfer of a child to another kindergarten, a copy of the health assessment results shall be provided upon request and without charge to the new kindergarten.

(c) Within 60 calendar days after the commencement of a new school year, the principal shall file a health assessment status report with the Department on forms developed by the Department and the Department of Public Instruction. The report shall document the number of children in compliance and not in compliance with G.S. 130A-440(a)."

NCGS § 143B – 147 Commission for Mental Health, Developmental Disabilities, and Substance Abuse Services — creation, powers and duties (Child Welfare and Protective Services) – "(a) There is hereby created the Commission for Mental Health, Developmental Disabilities, and Substance Abuse Services of the Department of Health and Human Services with the power and duty to adopt, amend and repeal rules to be followed in the conduct of State and local mental health, developmental disabilities, substance abuse programs including education, prevention, intervention, screening, assessment, referral, detoxification, treatment, rehabilitation, continuing care, emergency services, case management, and other related services. Such rules shall be designed to promote the amelioration or elimination of the mental illness, developmental disabilities, or substance abuse problems of the citizens of this State. The Commission for Mental Health, Developmental Disabilities, and Substance Abuse Services shall have the authority:

(1) To adopt rules regarding the a. Admission, including the designation of regions, treatment, and professional care of individuals admitted to a facility operated under the authority of G.S. 122C-181(a), that is now or may be established;

b. Operation of education, prevention, intervention, treatment, rehabilitation and other related services as provided by area mental health, developmental disabilities, and substance abuse authorities, county programs, and all providers of public services under Part 4 of Article 4 of Chapter 122C of the General Statutes;

c. Hearings and appeals of area mental health, developmental disabilities, and substance abuse authorities as provided for in Part 4 of Article 4 of Chapter 122C of the General Statutes; and

d and e. Repealed by Session Laws 2001-437, s. 1.21(a), effective July 1, 2002.

f. Standards of public services for mental health, developmental disabilities, and substance abuse services.

(2) To adopt rules for the licensing of facilities for the mentally ill, developmentally disabled, and substance abusers, under Article 2 of Chapter 122C of the General Statutes.

(3) To advise the Secretary of the Department of Health and Human Services regarding the need for, provision and coordination of education, prevention, intervention, treatment, rehabilitation and other related services in the areas of:

a. Mental illness and mental health,

b. Developmental disabilities,

c. Substance abuse.

d. Repealed by Session Laws 2001-437, s. 1.21(a), effective July 1, 2002.

(4) To review and advise the Secretary of the Department of Health and Human Services regarding all State plans required by federal or State law and to recommend to the Secretary any changes it thinks necessary in those plans; provided, however, for the purposes of meeting State plan requirements under federal or State law, the Department of Health and Human Services is designated as the single State agency responsible for administration of plans involving mental health, developmental disabilities, and substance abuse services.

(5) To adopt rules relating to the registration and control of the manufacture, distribution, security, and dispensing of controlled substances as provided by G.S. 90-100.

(6) To adopt rules to establish the professional requirements for staff of licensed facilities for the mentally ill, developmentally disabled, and substance abusers. Such rules may require that one or more, but not all staff of a facility be either licensed or certified. If a facility has only one professional staff, such rules may require that that individual be licensed or certified. Such rules may include the recognition of professional certification boards for those professions not licensed or certified under other provisions of the General Statutes provided that the professional certification board evaluates applicants on a basis which protects the public health, safety or welfare.

(7) Except where rule making authority is assigned under that Article to the Secretary of the Department of Health and Human Services, to adopt rules to implement Article 3 of Chapter 122C of the General Statutes.

(8) To adopt rules specifying procedures for waiver of rules adopted by the Commission.

(9) To adopt rules establishing a process for non-Medicaid eligible clients to appeal to the Division of Mental Health, Developmental Disabilities, and Substance Abuse Services of the Department of Health and Human Services decisions made by an area authority or county program affecting the client. The purpose of the appeal process is to ensure that mental health, developmental disabilities, and substance abuse services are delivered within available resources, to provide an additional level of review independent of the area authority or county program to ensure appropriate application of and compliance with applicable statutes and rules, and to provide additional opportunities for the area authority or county program to resolve the underlying complaint. Upon receipt of a written request by the non-Medicaid eligible client, the Division shall review the decision of the area authority or county program and shall advise the requesting client and the area authority or county program as to the Division's findings and the bases therefore. Notwithstanding Chapter 150B of the General Statutes, the Division's findings are not a

final agency decision for purposes of that Chapter. Upon receipt of the Division's findings, the area authority or county program shall issue a final decision based on those findings. Nothing in this subdivision shall be construed to create an entitlement to mental health, developmental disabilities, and substance abuse services.

(b) All rules hereby adopted shall be consistent with the laws of this State and not inconsistent with the management responsibilities of the Secretary of the Department of Health and Human Services provided by this Chapter and the Executive Organization Act of 1973.

(c) All rules and regulations pertaining to the delivery of services and licensing of facilities heretofore adopted by the Commission for Mental Health and Mental Retardation Services, controlled substances rules and regulations adopted by the North Carolina Drug Commission, and all rules and regulations adopted by the Commission for Mental Health, Mental Retardation and Substance Abuse Services shall remain in full force and effect unless and until repealed or superseded by action of the Commission for Mental Health, Developmental Disabilities, and Substance Abuse Services.

(d) All rules adopted by the Commission for Mental Health, Developmental Disabilities, and Substance Abuse Services shall be enforced by the Department of Health and Human Services."

NCGS § 90-109.1 – "(a) A person may request treatment and rehabilitation for drug dependence from a practitioner, and such practitioner or employees thereof shall not disclose the name of such person to any law-enforcement officer or agency; nor shall such information be admissible as evidence in any court, grand jury, or administrative proceeding unless authorized by the person seeking treatment. A practitioner may undertake the treatment and rehabilitation of such person or refer such person to another practitioner for such purpose and under the same requirement of confidentiality.

(b) An individual who requests treatment or rehabilitation for drug dependence in a program where medical services are to be an integral component of his treatment shall be examined and evaluated by a practitioner before receiving treatment and rehabilitation services. If a practitioner performs an initial examination and evaluation, the practitioner shall prescribe a proper course of treatment and medication, if needed. That practitioner may authorize another practitioner to provide the prescribed treatment and rehabilitation services.

(c) Every practitioner that provides treatment or rehabilitation services to a person dependent upon drugs shall periodically as required by the Secretary of the North Carolina Department of Health and Human Services commencing January 1, 1972, make a statistical report to the Secretary of the North Carolina Department of Health and Human Services in such form and manner as the Secretary shall prescribe for each such person treated or to whom rehabilitation services were provided. The form of the report prescribed shall be furnished by the Secretary of the North Carolina Department of Health and Human Services. Such report shall include the number of persons treated or to whom rehabilitation services were provided; the county of such person's legal residence; the age of such person; the number of such persons treated as inpatients and the number treated as outpatients; the number treated who had received previous treatment or rehabilitation services; and any other data required by the Secretary. If treatment or rehabilitation services are provided to a person by a hospital, public agency, or drug treatment facility, such hospital, public agency, or drug treatment facility shall coordinate with the treating medical practitioner so that statistical reports required in this section shall not duplicate one another. The Secretary shall cause all such reports to be compiled into periodical reports which shall be a public record."

NCGS § 131E-67 Specialty Hospitals – "All functions, powers, duties, and obligations heretofore vested in the Board of Directors of the North Carolina Specialty Hospitals and Eastern North Carolina Hospital are hereby transferred to and vested in the Department. All appropriations heretofore made to such Board of Directors or to any of the hospitals are hereby transferred to the Department. The Secretary of the Department shall have the power and duty to adopt rules for the operation of these facilities."

NCGS § 8-53. Communications between physician and patient.

"No person, duly authorized to practice physic or surgery, shall be required to disclose any information which he may have acquired in attending a patient in a professional character, and which information was necessary to enable him to prescribe for such patient as a physician, or to do any act for him as a surgeon, and no such information shall be considered public records under G.S. 132-1. Confidential information obtained in medical records shall be furnished only on the authorization of the patient, or if deceased, the executor, administrator, or, in the case of unadministered estates, the next of kin. Any resident or presiding judge in the district, either at the trial or prior thereto, or the Industrial Commission pursuant to law may, subject to G.S. 8-53.6, compel disclosure if in his opinion disclosure is necessary to a proper administration of justice. If the case is in district court the judge shall be a district court judge, and if the case is in superior court the judge shall be a superior court judge." (1885, c. 159; Rev., s. 1621; C.S., s. 1798; 1969, c. 914; 1977, c. 1118; 1983, c. 410, ss. 1, 2; c. 471.)

NCGS § 90-21.20B. Access to medical information for law enforcement purposes.

"(a) Notwithstanding any other provision of law, if a person is involved in a vehicle crash:

(1) Any healthcare provider who is providing medical treatment to the person shall, upon request, disclose to any law enforcement officer investigating the crash the following information about the person: name, current location, and whether the person appears to be impaired by alcohol, drugs, or another substance.

(2) Law enforcement officers shall be provided access to visit and interview the person upon request, except when the healthcare provider requests temporary privacy for medical reasons.

(3) A healthcare provider shall disclose a certified copy of all identifiable health information related to that person as specified in a search warrant or an order issued by a judicial official.

(b) A prosecutor or law enforcement officer receiving identifiable health information under this section shall not disclose this information to others except as necessary to the investigation or otherwise allowed by law.

(c) A certified copy of identifiable health information, if relevant, shall be admissible in any hearing or trial without further authentication.

(d) As used in this section, "healthcare provider" has the same meaning as in G.S. 90-21.11."

Related Federal Legal Drivers

45 CFR § 164.506 HIPAA: Consent for Treatment, Payment and Operations:

"(2) A covered healthcare provider may, without consent, use or disclose protected health information to carry out treatment, payment, or healthcare operations, if:

(i) The covered healthcare provider has an indirect treatment relationship with the individual; or

(ii) The covered healthcare provider created or received the protected health information in the course of providing healthcare to an individual who is an inmate.

(3)(i) A covered healthcare provider may, without prior consent, use or disclose protected health information created or received under paragraph (a)(3)(i)(A)-(C) of this section to carry out treatment, payment, or healthcare operations:

(A) In emergency treatment situations, if the covered healthcare provider attempts to obtain such consent as soon as reasonably practicable after the delivery of such treatment;

(B) If the covered healthcare provider is required by law to treat the individual, and the covered healthcare provider attempts to obtain such consent but is unable to obtain such consent; or

(C) If a covered healthcare provider attempts to obtain such consent from the individual but is unable to obtain such consent due to substantial barriers to communicating with the individual, and the covered healthcare provider determines, in the exercise of professional judgment, that the individual's consent to receive treatment is clearly inferred from the circumstances.

(ii) A covered healthcare provider that fails to obtain such consent in accordance with paragraph (a)(3)(i) of this section must document its attempt to obtain consent and the reason why consent was not obtained.

(4) If a covered entity is not required to obtain consent by paragraph (a)(1) of this section, it may obtain an individual's consent for the covered entity's own use or disclosure of protected health information to

carry out treatment, payment, or healthcare operations, provided that such consent meets the requirements of this section.
(5) Except as provided in paragraph (f)(1) of this section, a consent obtained by a covered entity under this section is not effective to permit another covered entity to use or disclose protected health information."

45 CFR § 164.514 (h)(1) Verification of Identity and Authority of Persons Requesting PHI

"(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart."

45 CFR § 164.510. Uses and disclosures requiring an opportunity for the individual to agree or to object.

CLIA 42CFR § 493.1291(f) Test results must be released only to ***authorized persons*** and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test.

CLIA 42 CFR § 493.2 "Authorized person**"** means an individual authorized under State law to order tests or receive test results, or both.

NC HISPC Reference Library

The NC HISPC team found the following websites and documents to be insightful.

Federal Health Information Technology Sites

US Department of Health and Human Services
http://www.hhs.gov/healthit/

Office of the National Coordinator on Health Information Technology

American Health Information Community
http://www.hhs.gov/healthit/community/background/

Privacy and Security

HIPAA
http://www.cms.hhs.gov/HIPAAGenInfo/

HIMSS HIPAA Compliance Survey
http://www.hipaadvisory.com/action/surveynew/results/summer2006.htm

North Carolina General Statutes
http://www.ncleg.net/gascripts/Statutes/StatutesTOC.pl

Community Health Information Exchanges, RHIOs

E Health Initiative
http://www.ehealthinitiative.org/

Nationwide Health Information Network (NHIN)

US Department of Health and Human Services NHIN
http://www.hhs.gov/healthit/healthnetwork/

NHIN Watch
http://nhinwatch.com/

Personal Health Records (PHR)

Markle Foundation Report on Consumers and PHR
http://www.connectingforhealth.org/resources/phwg_survey.pdf