

**Privacy and Security Solutions for Interoperable Health Information Exchange**

***North Carolina HISPC Interim Implementation Report***

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

Prepared by:  
Angie M. Santiago  
TM Floyd & Company for  
Holt Anderson,  
NCHICA, Inc.  
PO Box 13048  
Research Triangle Park, NC 27709

Submitted to:  
  
Linda Dimitropoulos, Project Director  
Privacy and Security Solutions for  
Interoperable Health Information Exchange

Research Triangle Institute  
P. O. Box 12194  
3040 Cornwallis Road  
Research Triangle Park, NC 27709-2194

February 13, 2007

## **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 Interim Implementation Report:

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

NC HISPC Co-Chairs  
James Murphy, NC DHHS MMIS  
Mike Voltero, BCBSNC  
Roy Wyman, Maupin Taylor Law  
David Kirby, Kirby Information Management  
Patricia Markus, Smith Moore Law

Contributors  
Donald Sweezy, Duke University Health System  
Sissy Holloman, UNC Hospitals

Solutions Work Group  
Legal Work Group

Editor  
Diana Gildea, Project Coordinator

### **NC HISPC Steering Committee**

Holt Anderson, NCHICA  
Phil Telfer, NC Governor's Office  
Linda Attarian, NC DHHS Division of Medical Assistance  
Wesley G. Byerly, Pharm.D., Wake Forest University Baptist Medical Center  
Fred Eckel, NC Association of Pharmacists  
Jean Foster, NCHIMA / Pitt County Memorial Hospital  
Donald E. Horton, Jr., LabCorp  
Eileen Kohlenberg, Ph.D., NC Nurses Association  
Mark Holmes, NC Institute of Medicine  
Linwood Jones, NC Hospital Association  
David Kirby, Kirby Information Management  
Patricia MacTaggart, Health Management Association  
Patricia Markus, Smith Moore Law  
Lawrence H. Muhlbaier, Ph.D., Duke University Health System  
James Murphy, NC DHHS Office of MMIS  
David Potenziani, M.D., UNC School of Public Health  
Melanie Phelps, NC Medical Society  
N. King Prather, BCBSNC  
Morgan Tackett, BCBSNC  
Mike Voltero, BCBSNC  
Roy Wyman, Maupin Taylor Law

## 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, 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, NCHICA, or by 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.

## Website Readers

During your visit to our Web site, your Web browser may produce pop-up advertisements. These advertisements were most likely produced by other Web sites you visited or by third party software installed on your computer. NCHICA does not endorse or recommend products or services that may appear as pop-up advertisements on your computer screen while visiting our site.

## Commercial Products or Services

Any mention of commercial products within the NC HISPC documents or web pages is for information only; it does not imply recommendation or endorsement of any commercial products, processes, or services by the State of North Carolina, NC HISPC, NCHICA, or by its members, board of directors, committees, or staff.

**Table of contents**

**Purpose ..... 1**

**Background ..... 1**

**Phase I Assessment ..... 2**

**Phase II Proposed Solutions..... 2**

**Phase III Implementation ..... 3**

    NC HISPC Solutions and Implementation Outline ..... 4

    Proposed CLIA Amendment..... 7

**Appendices ..... 10**

    Scenario Sub-groupings ..... 10

    Stakeholders Affected ..... 10

    Privacy & Security Domains ..... 10

    NC HISPC Reference Library..... 12

## **Purpose**

The NC HISPC Interim Implementation Plan Report consists of an implementation plan designed to address each of the solutions identified in the Interim Solutions Report using generally accepted project management and information security principles. We will introduce centralized processes which should be established when considering complex collaborative projects such as those we will propose in the Final Solutions Report.

The purpose of the NC HISPC Interim Implementation Plan Report is to document practical approaches and actionable steps for implementing solutions identified in the Interim Analysis of Solutions Report, and to create a framework to remove or mitigate the barriers identified while preserving essential privacy and security protections for consumers. Further, we will attempt to support the goal of interfacing with the Nationwide Health Information Network (NHIN) to permit widespread interoperability.

### Scope of Interim Implementation Plan

Implementation plans are based on the acceptance of a contract, project charter, and funding, none of which we have secured. We will design an adaptive implementation methodology for use in a hypothetical North Carolina Health Information Exchange.

It is our hope that the proposed solutions and implementations will generate collaborative health information technology projects within and around North Carolina. Due to the agreed statement of work, limited scope of the HISPC project, time and resource constraints, we will introduce suggested high - level implementation steps to the proposed solutions. Our suggestions within this implementation plan are not intended to constitute an "authoritative statement" under the State of North Carolina's policies, general statutes, and regulations. Nor does it bind the State of North Carolina, NC HISPC, NCHICA, its members, board of directors, committees, or staff, to implement the proposed solutions and implementation plan.

## **Background**

In April 2004, President George W. Bush issued an Executive Order articulating a vision for the future of healthcare in the United States. The President's plan included the formation of the American Health Information Community (AHIC), a federally-chartered advisory committee that provides input and recommendations to HHS on how to make health records digital and interoperable, and assure that the privacy and security of those records are protected in a smooth market-led way. The AHIC organized the Privacy and Security Workgroup that established the Health Information Security and Privacy Collaboration (HISPC) project in 33 states and Puerto Rico. In November 2006, the first phase of the NC HISPC project included an assessment that identified variations in privacy and security practices and laws affecting electronic health information exchange among various healthcare stakeholders in North Carolina. The initial findings may be found in the [Assessment of Variations Report](#) at the NCHICA website.

Following the assessment, the NC HISPC Solutions, Legal, and Implementations Workgroups and Steering Committee began the process of analyzing the findings and developing Interim Solutions to reduce or mitigate the barriers identified. The barriers and solutions are first centered on the fragmentation in health information processes and its supporting technology. Current health care practices are based on complex legislation and regulations and suffers from a hybrid of manual and automated processes that are confusing to practitioners and consumers. The premise for our solutions will be to design a collaborative approach to standardizing health care processes, its supporting technology, and developing an information technology project management framework to achieve the interoperability in a Nationwide Health Information Network (NHIN).

### Workgroups Composition

The Legal, Solutions, and Implementation Workgroups are comprised of practice managers, clinicians, professionals in public health policy, health information management, and information security attorneys who represent healthcare stakeholders or organizations specializing in privacy and security, laboratories, healthcare software vendors, and public health agencies.

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

## **Phase I Assessment**

### Assessment of Variations in Organization–Level Business Policies and State Laws

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

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.

Of the approximately 75 business practices submitted, 25 barriers have been identified and categorized as followed:

1. Range within organizations of misinterpretation and/or application of laws or regulation
2. Lack of business incentives to exchange information
3. Lack of policy standardization across entities
4. Lack of security standardization across entities
5. Lack of interoperability between processes and technology
6. Lack of workable technology
7. Conflicting or outdated federal or state laws or regulations.

## **Phase II Proposed Solutions**

### Summary of Interim Analysis of Solutions

During the initial planning phase, we considered the types of information requestors portrayed in the scenarios as well as the stated purpose of the health information exchange. The Variations Work Group clustered the scenarios into four sub-groups based on the purpose of the information exchanged, type of stakeholders to be interviewed, affected legal drivers, security domains relevant to the scenarios, and the subject matter resources required to analyze and propose the solutions to the identified barriers. The [four scenario sub-groups](#) are:

- |              |   |
|--------------|---|
| Sub-group 1: | Patient Care / RHIO (scenarios 1 - 4, 6)  |
| Sub-group 2: | Payment / Pharmacy Benefit Manager/ (scenarios 5, 7, 9, 10)   |
| Sub-group 3: | Secondary Use: Research, Operations, Marketing, Research, and HR Information (scenarios 7, 8, 11, 12, 14) |
| Sub-group 4: | Government, Public Health and Safety (scenarios 13, 15 -18)   |

The NC HISPC Interim Analysis of Solutions Report was the first round of ideas for solutions to the problems and/or ways to utilize opportunities associated with the appropriate and routine exchange of individual health information in electronic form in support of healthcare treatment, payment, operations, and other uses of electronic health information.

The Interim Analysis of Solutions Report also documented each of the identified potential solutions, their Health Information Exchange (HIE) context, privacy and security domains affected, stakeholders involved, HIE barriers being addressed, stage of development and use of solution and possible barriers to adoption.

Thirty-five solutions were submitted by the four sub-groups which have been mapped to the relevant barriers. Utilizing the vetting process detailed in the [Analysis of Interim Solutions Report](#), the solutions under consideration by the NC HISPC Solutions and Legal Workgroups, and Steering Committee are:

1. Establish a pilot project with adequate funding to explore the concept of the Person Oriented HIE.
2. Implement policy standards, such as model policy and legislation, to address the complexity and ambiguity surrounding the release of information.
  - a) Implement security standards to address the complexity and ambiguity surrounding the safeguarding of health information.
3. Implement sound business models to incentivize potential information sharing partners to participate in community based health information exchange.
4. Encourage greater collaboration between policy makers, subject matter, and technical experts to adopt HIE requirements.
5. Explore the dependencies between the business processes and their technical components for the purpose of interoperability.
6. Address the misinterpretation of laws or regulations by obtaining clarification and developing public and private awareness programs.
7. Amend conflicting Federal or State laws.

### **Phase III Implementation**

#### Implementation Plans for Identified Solutions Methodology

We began our implementation process by assigning a unique identifier to each barrier ensuring they were properly categorized and mapped to relevant solutions. The solutions submitted from the four sub-groups were also given unique identifiers. Duplicate or similar solutions were consolidated into one comprehensive solution.

During the solutions and legal workgroup sessions the need for standards harmonization emerged as a common theme among all four sub-groups. Our discussions included the need to build a Health Information Exchange framework incorporating interoperable policies, processes, and technology for the purpose of exchanging secure and timely health information within the state as well as across state lines. The groundwork would be laid by adopting project management standards that would establish centralized processes to plan, design, test, and implement health information technology projects that interface with the NHIN.

An important implementation strategy the HIE stakeholders should consider is to establish first a Project Management Office (PMO) to centralize and manage the multiple simultaneous complex projects. Benefits and features of a PMO are the development and implementation of sound project management methodology, documentation management, centralized project policies and templates, timelines, risk management, budget monitoring, communications across the project stakeholders, and the adoption of quality standards.

As we considered different approaches to developing our implementation plans, we determined that our project should start with cultivating a culture of health information technology standards in North Carolina. We adopted the project management methodology from Project Management Institute's Common Book of Knowledge which includes an internationally recognized framework to define, plan, execute, monitor and close projects in a manner that is risk-controlled, measurable, and orderly.

As we move forward with the assembling of stakeholders with differing requirements, incentives, philosophies, and approaches to exchanging health information, a centralized project management approach will improve the communications of such complicated collaborative projects, reduce project overhead, and diminish the risk of costly errors. Finally, the adoption of Health Information Exchange project management methodologies would not be limited to one state implementation plan but would integrate smoothly into a multi-state project.

### NC HISPC Solutions and Implementation Outline

All potential solutions and implementations that are submitted by members of the SWG, LWG and Steering Committee, will be documented in the NC HISPC ISWG Solutions and Implementation Worksheet. The ISWG Worksheet is designed to foster creativity among the submitters and ensure structure for the required documentation and deliverables.

The information contained in the ISWG Worksheet and how it will be used is as follows.

**HIE barrier addressed:** (PMO Use Only BR\_xx) The HIE barrier addressed includes the unique identifier and barrier type which can be traced to our original Variations Workgroup Assessment Tool Worksheet. At this point in the project, we have consolidated our barriers into the following major categories:

- Range within organizations of misinterpretation and/or application of laws or regulation
- Lack of business incentives to exchange information
- Lack of policy standardization across entities
- Lack of security standardization across entities
- Lack of interoperability between processes and technology
- Lack of workable technology
- Conflicting or outdated Federal or State Laws / Regulations

**Background:** The problem background includes a two or three paragraph description of the barrier which is being addressed in the proposed solution.

**Rationale for Solution:** Because multiple solutions may address the barrier, a rationale for proposing this particular solution over the alternatives are included in this 2 – 3 paragraph section.

**Solution:** The submitter will be asked to write a short paragraph describing each solution.

**HIE type (Groups 1 – 4):** The Health Information Exchange (HIE) type was derived by determining the purpose of the information and the parties involved in sending and receiving the requested information. We categorized our HIE types into four sub-groups: 1. Direct Patient Care, 2. Payer, 3. Secondary Use: Operations, Marketing, Research, Law Enforcement, and 4. State Government / Public Health.

**HIE model affected (E2E, PO HIE):** This section will describe how the proposed solution relates to the two HIE models we are exploring. In addition to the traditional model of exchanging health information from entity to entity (E2E), we will explore how the barriers and solutions would differ if the scenarios provided by RTI included the opportunity for the patient, or the person who was subject of the information, to have an active role in the exchange process. We will also consider how a Person Oriented Health Information Exchange (PO HIE) model, which was recently demonstrated by the Nationwide Health Information Network (NHIN) forum, may be further explored in North Carolina.

**Applicability of solution:** The applicability of the solution will attempt to identify the entities that would adopt and implement the solution.

**Stakeholders affected (1 – 18):** Although a solution may apply only to particular entities, it may affect various stakeholders. The stakeholders affected section of the implementation plan is based on the 18 stakeholder types provided by RTI. A complete list of the stakeholders may be viewed in the appendices section of this report [HISPC Stakeholders](#).

**Privacy & security domain(s)** addressed (1 – 9): The HIPAA Security Rule, 45 CFR §§ 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule which is applicable to the majority of our stakeholders and was effective in April 2005, laid the foundation for the adoption of information security standards. We will address these domains in one solution, the adoption of information security standards. A complete list of the domains may be viewed in the appendices section of this report [Privacy & Security Domains](#).

**Potential barriers / issues:** As community based health information exchanges continue to solidify, the implementation of risk management processes will identify potential barriers or issues to those exchanges and determine whether those barriers or issues are acceptable risks to the HIE or warrant mitigation strategies. Such barriers or issues which may need to be addressed could include but are not limited to competing interests, perception of increased risks to privacy, and its affects to persons who are incapable of making medical decisions.

**Phase of development** (Project Management and Security SDLC): Our implementation plans will include the current stage or phase within the Project Management and Systems Development Life Cycles (SDLC). When considering information security implementation standards we elected to utilize the standards developed for the Federal Information Systems and guides from the National Institutes of Standards and Technology (NIST). This will begin the process of solving the interoperability issues through the adoption of common criteria and to avail the stakeholders of the public documents and guidance available on the NIST website.

We have also taken the liberty to adjust the SDLC within the NIST Special Publication 800-64 document to include the business process that drives the supporting security requirement.

The Security SDLC phases are as followed:

1. **Initiation** - The initiation phase includes a needs determination and risk assessment which defines a problem that might be solved through automation and describes the security needs of the business process and its supporting technological component. This phase would include identifying and documenting the work flow process and mapping it to the supporting information system(s). Timeframe: 2 – 6 months depending on level of complexity.
2. **Development/acquisition** - This phase begins with a deeper analysis of the needs determination and risk assessment gathered during the Initiation phase. Formal documentation will include an analysis of laws and regulations, such as the Privacy Act, HIPAA, FISMA, OMB circulars, agency enabling acts, NIST Special Publications and FIPS, and other legislation and federal regulations, which define baseline security requirements. Timeframe: 2 - 6 months depending on level of complexity.
3. **Implementation:** The implementation phase includes the integration of the accepted security standards, awareness program, model policy, or legislation. Timeframe: 6 – 24 months depending on level of complexity.
4. **Operation/maintenance:** One of the concerns in the adoption of model policies, legislation and standards is how changes will be communicated to the stakeholders. In the information systems environment, this phase is focused on how systems modifications or enhancements would be developed, tested and implemented. To ensure that the model policies, legislation, and standards are current with the needs of the stakeholders, new legislation, and technology periodic reviews would be scheduled. In the event that a new risk or need is identified, the SDLC plan would be initiated. Timeframe: On-going.
5. **Disposition:** The disposition phase will refer to the closing of the contract and acceptance of the solution, policy, standard, or legislation. Timeframe: 12 – 36 months

NC HISPC will continue to explore the integration of the PMI and NIST SDLC methodologies to address the business process and its technological component in the HIE framework.

**Implementation plan:** It is our hope that the proposed solutions and implementations will generate collaborative health information technology projects within and around North Carolina. Due to the agreed statement of work, limited scope of the HISPC project, time constraints, and resources, we will introduce suggested high-level implementation steps to the proposed solutions. Our suggestions within this implementation plan are not intended to constitute an "authoritative statement" under the State of North Carolina's policies, general statutes, and regulations. Nor does it bind the State of North Carolina, NC HISPC, NCHICA, its members, board of directors, committees, or staff, to implement the proposed solutions and implementation plan.

**Implementation support:** The implementation support level designation is derived in two simple steps. First, we simply ask the stakeholders what their level of support is: high, medium, low. Second, we ask if their organizations would support this solution by adopting it into their own organizations, collaborating with their colleagues to promote the plan, or submitting a letter of support of their intention to implement the plan.

**Anticipated costs:** There are three components of costs to be aware of when considering a collaborative projects such as those we are proposing in our solutions. Cost estimating is a detailed estimate of the resources and tools necessary to conduct the activities of the project such as consultants, general counsel, administrative support, and collaborative project management tools. Cost budgeting aggregates the detailed estimates into packages to develop a cost baseline to monitor and control costs and identify funding requirements. The cost control process identifies positive or negative variances in the project's budget that can produce unacceptable levels of risk in the project and would need to be resolved. Once the need for a project is established during the initiation phase, such costs would be estimated and included in a Request for Proposal (RFP).

**Funding sources:** Funding sources will be identified once the need for a project has been established and costs have been estimated.

**Length of implementation:** Upon the initiation of a project, a project schedule will be drafted after identifying and sequencing project activities, prioritizing task dependencies, and estimating resources and work duration.

**Implementation complexity:** Determining the level of a project's complexity is crucial to identifying tasks, resources, and estimating costs or risks related to the project's activities. With the implementation of collaborative projects such as those that we are proposing, the level of complexity will range from medium to high.

**States affected:** As the project requirements are gathered during the initiation phase, the RFP or discovery team will need to conduct an initial assessment to determine the type of information to be exchanged, its mode of dissemination (paper or electronic), and whether the exchange route will be restricted within the state's border or will include interstate exchanges. Upon establishing the states affected by the HIE, a strategy for coordinating and overseeing the implementation of solutions will be developed by the Project Management Office (PMO).

## Sample Solution and Implementation Plan

### Proposed CLIA Amendment

#### **HIE barrier addressed: Conflicting or outdated federal or state law.**

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. **(PMO use only: Interim\_solution\_29 a)**

#### **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. **(PMO use only: Interim\_solution\_29 c)**

#### **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. **(PMO use only: Interim\_solution\_29 b)**

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

**HIE model affected:** Entity to Entity, Person Oriented HIE

**Applicability of solution:** To be determined by LWG

**Stakeholders affected:**

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 addressed:** To be determined

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

**Phase of development:** 2. Feasibility / planning

**Implementation plan:**

1. Obtain buy-in and letter of support from ACLA.
2. Inform and solicit support from AHIC, NCVHS, and other relevant bodies.
3. Engage the State E-health Alliance in the promotional efforts.
4. Receive endorsement of proposed CLIA amendments from HHS.
5. The NC HISPC stakeholders request CMS to issue proposed and final rules amending the CLIA regulations in accordance with one of the proposed alternative amendments.
6. CMS issues proposed and final rules amending the CLIA regulations.

**Implementation support:** High

**Anticipated costs:** Minimal or Unknown

**Funding sources:** N / A

**Length of implementation:** 18 months

**Implementation complexity:** Medium

**Affected states:** All

## Appendices

<u>Scenario Sub-groupings</u>	
Sub-group 1: Patient Care 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) 6. RHIO (Data Access)	Sub-group 3: Secondary Use 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 2: Payer 5. Payment (EHR Access) 9. Pharmacy Benefit A (Mail Order) 10. Pharmacy Benefit B (Claims Savings)	Sub-group 4: Government, Public Health & Safety 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)

### Stakeholders Affected

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. 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 (Specify)

### Privacy & Security Domains

1. Authentication: 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. Authorization: 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.
4. Transmission: Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.
5. Integrity: Information protections so that electronic personal health information cannot be improperly modified.
6. Event Audit: Information audits that record and monitor the activity of health information systems.
7. Safeguards: Administrative or physical security safeguards required to implement a comprehensive security platform for health IT
8. Data classification: State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

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

## **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/>

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 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](http://www.connectingforhealth.org/resources/phwg_survey.pdf)

### **National Institutes of Standards and Technology**

<http://www.nist.gov>

Implementing HIPAA Security:  
<http://csrc.nist.gov/publications/nistpubs/800-66/SP800-66.pdf>

Security Considerations in the Information SDLC  
<http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf>  
Building an Information Technology Security Awareness and Training Program

Recommended Security Controls for Federal Information Systems  
<http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf>

Engineering Principles for Information Technology Security  
<http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf>

Guide for Developing Security Plans for Federal Information Systems  
<http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>

**Project Management Institute**  
<http://www.pmi.org/info/default.asp>