Kentucky e-Health Privacy and Security Collaboration Final Report

Prepared by the Kentucky Cabinet for Health and Family Services, the University of Louisville and the University of Kentucky

April 17, 2007

Kentucky
UNBRIDLED SPIRIT™

Privacy and Security Solutions for Interoperable Health Information Exchange

Kentucky e-Health Privacy and Security Collaboration: Final Report

Subcontract No. 25-321-0209825
RTI Project No. 9825

Prepared by:

Cabinet for Health and Family Services
University of Kentucky
University of Louisville

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

April 10, 2007

Acknowledgements

The Kentucky Cabinet for Health and Family Services (CHFS) would like to thank all of the participants who freely gave of their time and expertise to assist the Kentucky e-Health Privacy and Security Collaboration. See Appendix A for a full list of project participants. Special thanks to the following project leaders and staff for their dedication:

Steering Committee Chairs

Robert Esterhay, MD, Chair, Health Management and Systems Sciences, University of Louisville School of Public Health

Carol Steltenkamp, MD, MBA, Chief Medical Information Officer, UK HealthCare, and Assistant Dean for Clinical Affairs, University of Kentucky School of Medicine

Working Group Chairs

Jeanne Reiners, Corporate IT Manager, Baptist Healthcare System
Chair of the Variations Working Group

Vickie Yates Brown, J.D., Member at Greenebaum, Doll & McDonald, PLLC
Chair of the Legal Working Group

Jeff Rose, Director of Technology Solutions at ConnectKentucky
Chair of the Solutions Working Group

Legal Services Contractor

Ned Benson, Attorney, and staff
Sturgill, Turner, Barker, Moloney

The Kentucky project team consisting of staff from the Cabinet for Health and Family Services, the University of Kentucky, and the University of Louisville were responsible for compiling this report. The recommendations and findings contained in this report do not necessarily reflect the views of the project participants or their organizations.

CHFS Project Staff

Trudi Matthews, Senior Policy Advisor and Project Director
Office of the Secretary

Linda Robinson, IT Systems Consultant
Office of Information Technology

Smita Prasad, Intern
Office of Health Policy

Richard Stout, Intern
Office of Health Policy

University of Louisville Project Staff

Robert J. Esterhay, M.D., Associate Professor and Chair
Department of Health Management and Systems Sciences
School of Public Health and Information Sciences

Susan Olson-Allen, Ph.D., Project Coordinator
Department of Health Management and Systems Sciences
School of Public Health and Information Sciences

Bruce W. Edwards, B.S., Information Security Officer

Marti Arvin, J.D, Privacy Officer

University of Kentucky Project Staff

Carol Steltenkamp, MD, MBA, Chief Medical Information Officer, UK HealthCare, and Assistant Dean for Clinical Affairs, University of Kentucky School of Medicine

Julia F. Costich, J.D., Ph.D., Chair
Department of Health Services Management
College of Public Health

Carol L. Ireson, R.N., Ph.D., Associate Professor
College of Public Health

Table of Contents

	Page
Executive Summary	**1**
1.0 Background	**5**
2.0 Purpose and Methodology	**12**
3.0 Assessment of Variations Findings	**19**
4.0 Summary of Key Findings from the Assessment of Variation	**32**
5.0 Overview of Solutions Identification and Assessment	**36**
6.0 Summary of State Proposed Solutions	**47**
7.0 Interstate Health Information Exchange and National-level Recommendations	**48**
8.0 Conclusions and Next Steps	**48**

Appendices

A: Steering Committee & Working Group Members

B: Health Information Exchange Scenarios

Executive Summary

Health care is the only industry of its size still dominated by paper, phone, fax, and mail. Most American clinicians still rely on file folders with handwritten notes, paper prescriptions, and incomplete patient histories stored in file cabinets. While patients and physicians benefit from sophisticated technology to diagnose and treat disease, the relatively basic information technology necessary to record, store, share and protect health information electronically remains the exception not the rule.

In Kentucky, rising health care costs, concerns over access to quality, affordable care and poor health outcomes led a bipartisan group of leaders in the General Assembly and officials in Governor Fletcher's Administration to work together on e-Health as a solution.

On March 8, 2005, Governor Fletcher signed Kentucky's landmark e-Health legislation, known as Senate Bill 2 (SB2), authorizing the creation of a secure, interoperable statewide electronic health network. SB2 also created the Kentucky e-Health Network Board to oversee e-Health efforts in the state. Led by clinical leaders from Kentucky's two major research universities – the University of Louisville (U of L) and University of Kentucky (UK) – the e-Health Board consists of a number of public and private sector health leaders and is attached to the Cabinet for Health and Family Services (CHFS).

Kentucky e-Health Privacy and Security Collaboration

One of the first projects undertaken by the e-Health Board was the **Kentucky e-Health Privacy and Security Collaboration**. In May 2006, Kentucky was one of 33 states awarded a contract to participate in the Health Information Security and Privacy Collaboration (HISPC), a federally-funded collaboration involving the Office of the National Coordinator, the Agency for Healthcare Research and Quality, RTI, and the National Governors Association. Governor Ernie Fletcher designated CHFS as the project manager but requested that CHFS staff to work collaboratively with faculty from U of L and UK on the project.

Under federal contract requirements, Kentucky was responsible for organizing a large group of Kentucky stakeholders to participate in a number of Working Groups and committees with specific responsibilities for portions of the project:

- a **Steering Committee** to oversee the project and develop a plan for implementing recommendations for Kentucky
- a **Variations Working Group** to assemble organization-level business practices related to the confidential and secure exchange of health information
- a **Legal Working Group** to analyze barriers to information exchange and map those barriers back to applicable law and regulation
- A **Solutions Working Group** to develop an inventory of possible approaches to dealing with any barriers or other challenges identified.

Kentucky's e-Health Privacy and Security Collaboration Stakeholder Community consisted of more than 60 volunteers and staff from a wide variety of stakeholder organizations and backgrounds. For a complete list of participating stakeholders, see Appendix A.

This report is a result of this nearly yearlong collaborative project. The goal of the project is to assess at the state and local levels how privacy and security practices and policies affect health information exchange (HIE). The main objective of this report is to outline the findings from the assessment of variations in business policy and practice and to provide an overview of various solutions and functional steps possible to address the privacy and security issues that may affect and impede health information exchange in Kentucky.

Findings and Recommendations

For technology to improve the efficiency and quality of health services to the greatest degree possible, health information exchange must be largely instantaneous and automatic. This ability is facilitated largely by the use of a set of recognized rules or standards among organizations, including standards for protecting the privacy and security of the information. This project produced a number of important findings and recommendations regarding the challenges related to various health information exchange situations, including:

- **Widespread misunderstanding and confusion concerning state and federal laws relating to the privacy and security of health information**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provided baseline protections for health information across the United States, but other state and federal laws also contain provisions regarding the privacy and security of protected health information (PHI). Project participants expressed great concern regarding the large number of differing standards and interpretations between state and federal laws protecting health information. Multiple state or federal laws and regulations that deviate significantly from the baseline privacy and security protections that HIPAA provides can be particularly problematic in an electronic information environment.

Health care providers and practitioners in particular expressed a great deal of uncertainty about when patient data may be released and to whom. Issues arose regarding the release of information to payers for administrative purposes as well as for organizations to monitor patient management. Release of information for non-medical purposes, such as to police, parents of adult children, employers, marketers and government agencies were also particularly problematic.

- **Issues related to handling of sensitive protected health information**

Particularly sensitive areas of protected health information include information related to mental health, substance abuse, HIV/AIDS, sexually transmitted diseases and some other communicable diseases. These types of sensitive conditions are afforded special

protections due to the stigma and potential negative consequences of inappropriate information disclosure. While agreeing that special protections for sensitive health information are important, project stakeholders also noted the difficulty of ensuring compliance with all the provisions found throughout state and federal law related to sensitive PHI. The differing provisions and standards for appropriate disclosure means that, when in doubt, health organizations do not share any health information. However, this policy could affect greatly both the continuity of care and the quality of care provided as electronic health information exchange becomes customary. Some participants urged the development of a more coherent set of standards around sensitive PHI. Such standards could have two positive benefits: 1) ensuring to a greater degree that sensitive PHI is afforded the special protections it deserves and 2) making it easier for health organizations to comply with the law.

- **Technology limitations related to electronic information exchange**

The project examined many limitations to currently available health information technology. Identity management is an issue for any technology application, but it is especially important with health information where life and death matters are at stake. Determining policies and practices for appropriate access, authentication, authorization, and auditing for information systems are critical to protecting the privacy and security of electronic health information. In addition, interoperability is a critical issue to health information exchange because health information systems currently cannot easily communicate with one another. The lack of a standard way to match patient records across health organizations is another technology challenge. Finally, there are associated problems with the various types of data transfer and ensuring secure transmission.

- **Relative silence in law on health information exchange**

Much of Kentucky law and regulation governing health care and public health assumes and reinforces a paper-based environment rather than an electronic environment for health information management. Emerging practices such as e-prescribing, health information exchange, RHIOs, and personal health records are so new and dynamic that clear legal parameters simply do not exist yet. Without clear policy guidance, health organizations may be reluctant to move aggressively into the world of e-Health. In some cases, law and regulation may simply be out-dated and have not changed in decades to reflect current practices. The process of updating privacy and security statutes and regulations is difficult because these statutes and regulations are scattered throughout state codes.

- **Concern regarding business risk and adverse legal action if information exchanged**

The ambiguities between state and federal law, the current limitations to technology and the “newness” of e-Health mean that there are inherent risks to early adopters of health information technology and exchange. While many providers, administrators and practitioners have managed to deal with these challenges, there is an underlying

concern that a specific situation may uncover hidden problems, thus exposing health care entities to unanticipated risk to both their business reputations and to adverse legal action.

A number of solutions were proposed by stakeholders as ways to address the issues and challenges identified through this project. A key means to address the issues and implement proposals will be through the statutorily-required Privacy and Security Committee of the e-Health Network Board. This committee will be appointed by the e-Health Board in April 2007 and charged with addressing the issues identified by this report and implementing recommendations a state Implementation Plan (forthcoming). Several categories of action defined in the report address:

- **Statutory solutions** requiring the review, revision, or amendment of state or federal laws that are inconsistent with related provisions in state or federal law, threaten the feasibility of HIE, or are subject to widespread uncertainty and misinterpretation.

- **Regulatory solutions** in areas where regulations may be modified or clarified to facilitate HIE, including confusion or conflict between state and federal regulation and ambiguities that lead to fear of violating a regulation, with associated sanctions or litigation.

- **Administrative or organizational solutions** to amend, create, and standardize health care providers' administrative actions, business policies and practices that arise because of organizational custom and variation in organizational policies and practices.

- **Technological solutions** to improve the secure transmission of health information, improve professional competence regarding the nature and use of digital or electronic communication, and increase the adoption of HIT.

- **Public awareness and education solutions** promote training and education of consumers, health care providers, government officials, professional associations, employers, public officials, researchers, and educators about the rules governing HIE, the benefits to electronic HIE, and their respective rights and obligations regarding enhanced quality of care. These solutions address the low level of education about HIE and privacy and security laws as well as provider concern about business reputation and public relations issues.

1.0 Background

1.1 Overview and Background of e-Health and the role of privacy and security

Health care is the only industry of its size still characterized by repeated and costly phone calls, faxes, and mail. Most American clinicians still rely on file folders with handwritten notes, paper prescriptions, and incomplete patient histories stored in file cabinets. While patients and physicians benefit from extremely sophisticated diagnostic technology in the U.S., the relatively basic information technology necessary to record, store, share and protect health information electronically remains largely unavailable.

The need for the health care industry to move to electronic systems has been well established over the past few decades. Recently, a number of the factors have accelerated the pace of change on the national level leading health care providers, clinicians and policy makers to look to technology for solutions to health problems. The Hurricane Katrina disaster that wiped out overnight thousands of paper medical records demonstrated how vulnerable paper records are to destruction. Growing concern over inconsistent quality of care and medical errors has placed pressure on health care leaders and policy makers for solutions.

In Kentucky, rising health care costs, concerns over access to care and poor health outcomes have also been drivers of change. Kentucky families have experienced high growth in health insurance costs, which has driven up Medicaid rolls and increased the number of uninsured. Kentucky also has higher than average rates of chronic disease, obesity, smoking and disability. Issues of affordability and access coupled with the poor health status of Kentucky's population have led Governor Ernie Fletcher, a former family physician, to lead the charge for improved health and wellness and better information for Kentuckians to control health care costs, improve quality and lead healthier lifestyles. The Governor, members of the General Assembly and health care leaders looking for economic advancement have also played a large role in the move toward using technology to transform health care cost and quality while at the same time improving the economic outlook for Kentucky.

Recognizing these needs and concerns, a bipartisan group of leaders in the Kentucky General Assembly and officials in Governor Fletcher's Administration worked to pass e-Health legislation. On March 8, 2005, Governor Fletcher signed Kentucky's landmark e-Health legislation, known as Senate Bill 2 (SB2), which called for the creation of a secure, interoperable statewide electronic health network. SB2 also created the Kentucky e-Health Network Board, attached to the Cabinet for Health and Family Services, to oversee e-Health efforts in the state.

One of the most fundamental challenges to electronic health information exchange is how to protect the privacy and security of an individual's health information. While large numbers of Americans – nearly two-thirds in a recent Harris poll - support the use of electronic health records, privacy and security top the list of concerns with the move toward e-Health. On the other hand, health professionals looking to adopt or further the

use of health information technology and exchange cite the complex web of state and federal privacy and security laws and regulations as one of the biggest barriers to progress toward a truly interoperable environment. Ensuring the privacy and security of protected health information in an electronic environment is critical to creating public trust and support for e-Health, ensuring providers have access to clinical information without jeopardizing their information systems or increasing their liability risk, and achieving the efficiencies necessary to improve care and affordability. As more and more health entities move to electronic health records and health information exchange, a robust examination of privacy and security practice and law is needed to ensure public trust and continued private sector innovation.

1.2 Description of e-Health development in Kentucky

In Kentucky, the passage of SB2 in 2005 ignited interest and established the structures for furthering e-Health. In addition to creating a Board of public and private sector leaders, the legislation also established the Healthcare Infrastructure Authority, a partnership of Kentucky's two major research universities – the University of Kentucky (UK) and the University of Louisville (U of L) – to provide leadership for the Board. The Cabinet for Health and Family Services, at the urging of Governor Fletcher, has taken a leading role in fostering e-Health in the state by providing staff support to the Board and working with the Board leadership from UK and U of L.

Kentucky's e-Health efforts face a challenging environment. The first challenge is the low level of investment in technology and e-Health relative to other states. Adoption rates for electronic medical record systems, e-prescribing, and other forms of health information technology are currently low in the state. A study done by the Kentucky Medical Association in 2003 found, for example, that only 59 percent of physician practices with electronic medical records systems have the connectivity to communicate prescriptions to a pharmacy electronically. In 2003, also, a University of Kentucky study estimated that Kentucky physicians are roughly on par with national averages for adoption of electronic medical records but that number is still below 25 percent of physicians.

It is not enough, though, to have clinicians and providers use health information technology in the care environment. To achieve a lower cost, higher quality health care system and to improve health outcomes, the information that resides in electronic health records must be exchanged securely and confidentially when appropriate between organizations. With health information exchange, better and more complete clinical information would be available at the point of care thereby reducing duplicate tests and prescriptions, avoiding harmful drug interactions and improving quality of care. Electronic health information exchange could also reduce significantly administrative costs by reducing the current labor-intensive use of fax, mail and phone associated with paper medical records.

Thus, another challenge for Kentucky is developing the infrastructure necessary to allow the interoperable exchange of health information. Currently, in addition to Kentucky's

statewide e-Health efforts, three regional health information organizations (RHIOs) or health information exchanges (HIE) currently exist within Kentucky with differing levels of maturity. One active RHIO, HealthBridge, located in northern Kentucky and the greater Cincinnati area is one of the nation's longest running and most financially viable community e-Health efforts. Both the Louisville Health Information Exchange (LouHIE), and the Northeast Kentucky RHIO located in Morehead, Kentucky, began in 2006 and are moving aggressively through planning stages toward developing robust business models.

Kentucky has approximately four million residents dispersed across very diverse geographic areas and health care markets. A particular challenge will be whether Kentucky has the critical mass of participation across its health care markets to be able to sustain financially and organizationally the development of additional RHIOs or HIE efforts. Each of the current local initiatives is working with the e-Health Board to explore ways to share infrastructure investment and to foster collaboratively the development of e-Health in Kentucky to ensure strategic use of resources.

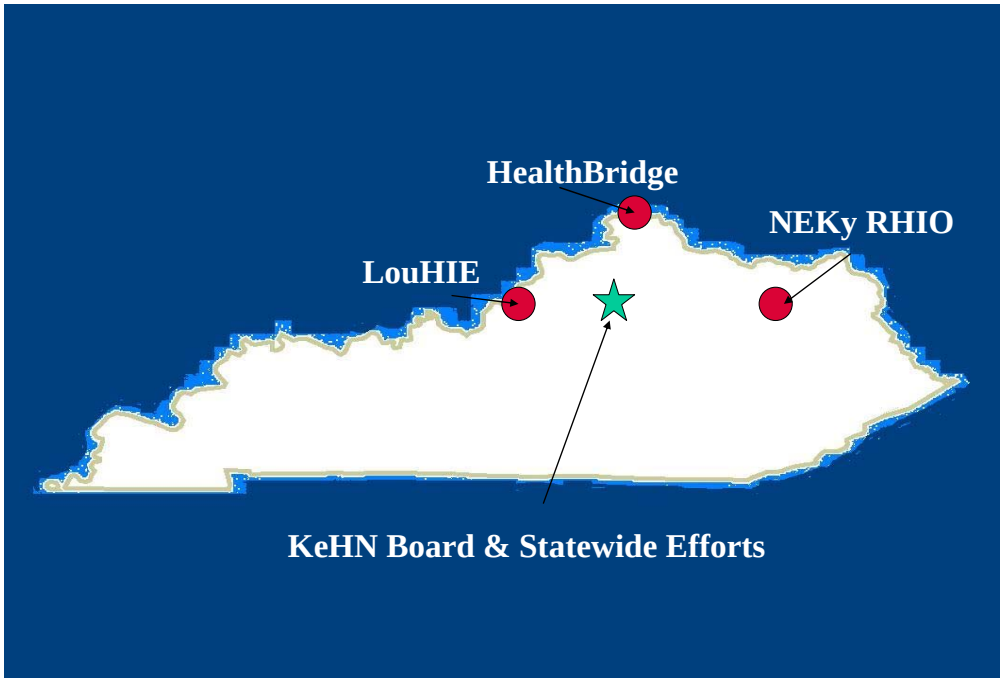
While only a few local health information exchange efforts are underway in Kentucky, there are other notable examples of e-Health efforts in the state including the Veterans Health Administration, the Kentucky Department of Corrections electronic medical record system, and the Kentucky All Schedule Prescription Electronic Reporting system (eKASPER). The Kentucky e-Health Network Board provides a statewide coordinating structure to be able to utilize strategically, available resources to develop a secure statewide Kentucky e-Health Network that can also participate in the national e-Health effort.

Kentucky RHIOs & Local HIE Efforts

- **HealthBridge** is a nationally recognized health information exchange serving the Greater Cincinnati area, including several counties in Northern Kentucky. Formed in 1997, HealthBridge is the largest community-based clinical messaging system in the country. By working with all participating healthcare stakeholders, HealthBridge is facilitating an integrated and interoperable electronic community healthcare system. HealthBridge delivers electronically over 1.4 million results (laboratory, radiology, transcription and ADT) to over 4,000 physicians each month. HealthBridge provides access to over 60 hospital-based critical care systems including radiology images, fetal heart monitoring, hospital-based electronic medical records and chart completion, among others. While health care in the rest of the country is still dominated by paper, phone and fax, HealthBridge has changed the care environment in the Greater Cincinnati and Northern Kentucky area, making e-Health an everyday reality.

- **Louisville Health Information Exchange (LouHIE)** is a new Regional Health Information Organization (RHIO) in the Greater Louisville area. Established in January 2006, LouHIE was the result of two years of research and effort by faculty of the University of Louisville. LouHIE has grown into a community-wide effort encompassing a broad set of stakeholders, including representatives from payers, providers, practitioners and consumers. LouHIE's goal is to lower costs and improve health care in the community and is currently exploring the development of a community health record bank as the model for health information exchange in the community.

- **Northeast Kentucky RHIO** is a partnership between Morehead University, Northern Kentucky University and St. Claire Regional Medical Center. Currently under development, the Northeast Kentucky RHIO seeks to establish a health information exchange that serves the northeastern Kentucky region.



1.3 Kentucky e-Health Projects

After completing its assessment and administrative organization in 2005, the Kentucky e-Health Board undertook several critical breakthrough efforts necessary for the development of e-Health in Kentucky.

- **Kentucky e-Health Privacy and Security Collaboration**

Kentucky was one of 33 states awarded a contract to participate in the Health Information Security and Privacy Collaboration (HISPC), a federally-funded collaboration involving the Office of the National Coordinator, the Agency for Healthcare Research and Quality, RTI, and the National Governors Association. Beginning in May 2006, the Cabinet for Health and Family Services (CHFS) served as the project lead and collaborated with the University of Louisville and the University of Kentucky on key deliverables. The goal of the project is to assess at the state and local levels how privacy and security practices and policies affect health information exchange (HIE).

This report is one of the major deliverables from the Privacy and Security Collaboration. More about the scope, purpose, methodology and findings of the project are provided in subsequent sections of this report.

- **Kentucky Health Information Partnership (K-HIP)**

One of the first major projects undertaken by the e-Health Board was the discussion regarding the use of claims information and simplification of administrative transactions. Upon the advice of e-Health experts in Kentucky and nationally, Secretary Mark Birdwhistell of the Kentucky Cabinet for Health and Family Services convened a group of payors and other stakeholders in health care to explore interest in working together on a statewide e-Health initiative. Secretary Birdwhistell indicated that Medicaid was interested in developing a claims-based health record for its members and invited other partners to join the Cabinet and the e-Health Board in pursuing this project as a statewide e-Health initiative.

In August 2006, the Cabinet, on behalf of the group, presented a concept paper to the Kentucky e-Health Network Board that proposed joint development of a statewide internet portal with two main areas of functionality: a clinical site that could deliver to providers a patient health summary based on claims data and an administrative site for conducting standard administrative transactions across all plans, such as claims submission and eligibility and benefits verification (see Table below). This initiative was designated the Kentucky Health Information Partnership or K-HIP. In January 2007, Kentucky was awarded $4.9 million from the Centers for Medicare and Medicaid Services through a Medicaid Transformation Grant to develop K-HIP.

The state is moving forward with a broad group of stakeholders to implement this project. Project plans call for the development of a common payor-provider web portal with the capacity for access to patient health information and single-sign on access for administrative transactions. Initial estimates of cost savings to Kentucky exceeded $40 million dollars. Using data from nearly all the major payors in Kentucky, K-HIP would have information for as many as 60 percent of Kentucky's 4 million residents, including Medicaid's 710,000 enrollees, the 135,000 enrolled in the Passport managed care plan in Louisville; 231,000 Kentucky state employees; and more than a million of Kentucky's privately insured residents.

Table 1: Proposed Functions and Information Available through the K-HIP Web Portal	
CLINICAL INFORMATION:	**ADMINISTRATIVE INFORMATION:**
• **Rx history** - including medication – identified by national drug code; date prescription filled; days of supply • **Provider service information** – including outpatient, inpatient, and emergency room visit information with name of the treating provider, place of service, date of visit, reason for the visit, procedures performed during the visit, and provider phone, city, and state • **Diagnosis codes** - including diagnosis, dates patient received care for this diagnosis, the place of service, and the doctor • **Lab and diagnostic test history** - type of lab/test performed, date lab/test performed, place of service and doctor ordering • **Immunizations**– immunization, date performed • **Patient information –** such as name, date of birth, age, gender, address, and phone	• **Request for eligibility verification** • **Submission of request for pre-authorization** • **Check status of prior authorization request** • **Submission of new medical claims** • **Check status of submitted claims**

- **The e-Prescribing Partnerships in Kentucky (ePPIK) Grant Program**

e-Prescribing is widely viewed as an important early win that can drive adoption of health information technology by physicians and increase the efficiency and safety of health care. CHFS in partnership with the e-Health Board and the Governor's Office for Local Development will fund adoption of health information technology to advance e-Prescribing in the Commonwealth. The e-Prescribing Partnerships in Kentucky (ePPIK) Grant program will provide funding for physician offices and clinics that want to purchase HIT software that includes e-Prescribing capability. In addition, the ePPIK grant program will promote the formation of partnerships within a community between physician offices, hospitals, pharmacies, and other health care entities to facilitate true end-to-end electronic prescription processing.

A total of $300,000 in funding for the ePPIK grant program comes from the Foundation for a Healthy Kentucky and the Hal Roger's Grant Program within CHFS that supports the Kentucky All Schedule Prescription Electronic Reporting (eKASPER), the nation's premier program to monitor prescription drug abuse of controlled substances. These two sponsors are interested in improving health care in Kentucky and learning how e-Prescription adoption will affect the KASPER program.

The Governor's Office for Local Development will serve as the administrator of the grant under the direction of CHFS. Grant applicants are required to match grant funds with their own investment. Governor Fletcher announced awards ranging from $10,000 to $81,000 to five partnerships around the state in January 2007.

- **Annual Kentucky e-Health Summit and Annual Report**

Because of the highly collaborative nature of e-Health, one of the critical needs in Kentucky is to inform, inspire action, and discuss critical needs and challenges among a broad cross-section of stakeholders about the progress of e-Health and the work of the KEHN Board.

The KEHN Board hosted its first statewide e-Health Summit in January 2007 as a means to bring together payors, providers, consumers, and other interested stakeholders to learn about and discuss the development of e-Health in Kentucky. A number of prominent national speakers and state leaders appeared including National Health Information Coordinator, Dr. Robert Kolodner, and Governor Ernie Fletcher. At the Summit, the KEHN Board released its first Annual Report, providing an overview of its initial assessment of the e-Health landscape and critical recommendations for moving e-Health forward.

In addition to these key accomplishments, the KEHN Board also seated an advisory group of technical and clinical experts to assist with the development of a long-term strategy for e-Health in Kentucky. The Kentucky e-Health Action Plan is the culmination of months of deliberation and discussion by the e-Health Advisory Group under the KEHN Board's direction.

- **e-Health Advisory Group and Action Plan**

In July 2006, the Board appointed an advisory group of HIT experts, clinicians, and representatives from within the state-based RHIOs to assist with the long-term planning needed for the statewide initiative. The Board chairs gave the Advisory Group the charge of developing an action plan for how Kentucky would establish a statewide e-Health network with the goals of containing health care costs, improving quality of care and health outcomes and creating economic development opportunities in Kentucky. The advisory group is working to develop a comprehensive five-year action plan for the development of statewide health information exchange in Kentucky and anticipates releasing its report in Spring of 2007.

2.0 Purpose and Methodology

2.1 Description of the purpose and scope of this report

Establishing an efficient and effective interoperable health information exchange in Kentucky is a top priority, and Kentucky stakeholders on the Kentucky e-Health Network Board and its various groups and committees are working diligently to confront the barriers to adopting health information technology.

This report is a result of the nearly yearlong Kentucky e-Health Privacy and Security Collaboration. The goal of the project is to assess at the state and local levels how privacy and security practices and policies affect health information exchange (HIE). The main objective of this report is to outline the findings from the assessment of variations in business policy and practice and to provide an overview of various solutions and functional steps possible to address the privacy and security issues that may affect and impede health information exchange in Kentucky.

2.2 Methodology for the Kentucky e-Health Privacy and Security Collaboration

Kentucky Governor Ernie Fletcher designated CHFS as the applicant and project manager for the Kentucky e-Health Privacy and Security Collaboration under the auspices of the Kentucky e-Health Network Board. Kentucky's e-Health Privacy and Security Collaboration project management team consisted of staff from the Cabinet for Health and Family Services (CHFS), the University of Louisville School of Public Health and Information Sciences (U of L) and the University of Kentucky (UK).

Each organization had a specific role and set of duties related to the project. CHFS was responsible for overseeing the project and staffing the Steering Committee and the Legal Working Group. In addition, CHFS engaged a law firm to develop a compendium of state e-Health privacy and security laws and assist the Legal Working Group with barrier mapping. The University of Louisville staff was responsible for the Variations

Assessment process, the Variations Working Group and preparation of the Variations Report. University of Kentucky staff was responsible for the Solutions Analysis and the Solutions Working Group. The Steering Committee co-chairs, Drs. Robert Esterhay (U of L) and Carol Steltenkamp (UK), come from each of the universities involved in the project and are also the project managers for their respective university's deliverables.

Prior to award of the contract, CHFS staff began extensive outreach through the Kentucky e-Health Network Board, university contacts and state government to develop a list of potential stakeholders who would be interested in being involved in this project. After being awarded the Privacy and Security contract in May 2006, CHFS determined, due to the tight timeframes for the project, to recruit a member for nearly every stakeholder group related to health care privacy and security issues to be involved. This helped to ensure business practices were collected and categorized appropriately from the beginning of the project and to mitigate the need for extensive outreach to additional stakeholders.

Under federal contract requirements, Kentucky was responsible for organizing stakeholders to participate in a number of Working Groups and committees:

- a **Steering Committee** to oversee the project and develop a plan for implementing recommendations for Kentucky
- a **Variations Working Group** to assemble information on organization-level business practices
- a **Legal Working Group** to analyze barriers to information exchange and map those barriers back to applicable law and regulation
- A **Solutions Working Group** to develop an inventory of possible approaches to dealing with any barriers or other challenges identified.

Kentucky's e-Health Privacy and Security Collaboration project Stakeholder Community consisted of more than 60 volunteers and staff from a wide variety of stakeholder organizations. In addition, the involvement and oversight of the project by the Kentucky e-Health Network Board has allowed additional stakeholder involvement and input into the project. The Steering Committee consists of 12 members and is chaired by physician faculty members from U of L and UK. Additional members of the Steering Committee consist of the three working group chairs as well as physician, health plan, hospital, state government, privacy and security experts, and consumer representatives. The Variations Working Group is comprised of 27 members with a broad range of stakeholder groups providing input into the development of the business practices including privacy and security officials, technology experts, clinicians and staff from several hospitals, a health plan, the local health department association, a community health center, long term care facilities, physician and physician office managers from several physician practices and clinics, nurses, state government, the quality improvement organization, pharmacists association, consumer, lab, department of corrections and academia. The Legal Working Group includes 11 attorneys from the state medical association, hospitals, academia, health plans, state government, an employer, and law firms with health or privacy and security expertise. The Solutions

Working Group consists of 11 members including chief information officers and policy experts from hospitals, academia, a health plan, state government, and technology companies. In addition to the broad stakeholder representation in the stakeholder community, the individuals involved in Kentucky's project bring together some of the state's leading minds in e-Health and privacy and security issues with expertise in clinical practice, privacy and security policies and law, RHIO and health information exchange efforts, public health informatics and clinical information systems.

The federal contractor for the project, RTI, provided training to staff on the project. As mentioned previously, RTI's data collection process required states to use a list of 18 scenarios that provided a variety of situations involving health information exchange among organizations (See Appendix B). The volunteers involved on the various groups were to deliberate on the scenarios and discuss what business practices would be used in Kentucky for health information exchange to occur. Then working groups would analyze the legal and regulatory issues involved, identify solutions for barriers to information exchange, and develop an implementation plan for the state. The project team from CHFS, UK and U of L determined that having an initial in-person retreat would likely be the best way to help all members of the stakeholder community understand the nature and purpose of the project and devote the concerted intellectual effort needed to develop the business practices.

- **Assessment of Variations Process**

Staff conducted initial orientation calls in July 2006 with the Steering Committee, Variations and Legal Working Groups to discuss their work and timelines and to invite stakeholders to participate in the project retreat. The Kentucky Privacy and Security Retreat was convened on August 2, 2006, at the University of Louisville's School of Public Health and Information Sciences. Members of the entire Kentucky e-Health Privacy and Security stakeholder community were invited to attend, not just the Variations Working Group. More than 50 stakeholders and project staff participated in the retreat. Attendees were divided into four groups based on stakeholder area. Each group was given four to five scenarios to discuss and was assigned a facilitator and scribe from the project staff to assist the group and capture the business practices that emerged from the discussion. The entire group came back together to discuss the bioterrorism scenario and to share the results of their discussions. Following the retreat, staff entered the information for each group into a database and refined the information collected. The retreat generated more than 125 business practices.

At the end of August, once the business practice information was collected and refined, staff asked the Variations Working Group as well as attendees at the retreat to fill in any gaps and provide additional information where necessary. To keep the review and comment process manageable, respondents were asked to review only the business practices entered for their group and respond via email with their comments to their group facilitator. Unfortunately, few additional comments were received.

At the beginning of September, the project team decided to hold a series of additional conference calls with the Variations Working Group members to collect supplemental information. The Variations Working Group met for three conference calls of approximately two hours each over the course of three weeks in September and October. During the calls, the scenarios and business practices were presented to the entire group rather than a specific subset to ensure broad opportunity for comment and feedback. Project staff from U of L facilitated the calls, reading through each scenario briefly with attendees, going through information collected, asking for the appropriateness of categorizations, and gleaning additional information about how information is exchanged. Following the conference calls, staff captured the changes and entered them to the database/spreadsheet.

During July and August of 2007, staff from the law firm Sturgill, Turner, Barker and Moloney (STBM) worked under contract with CHFS to compile a comprehensive listing of e-Health-related and privacy and security law. Based on its compilation, STBM staff was responsible for analyzing any business practices identified as barriers and performing an initial map of the practice back to state or federal law. The Legal Working Group met in a series of conference calls between August and October 2006 to review business practices collected by the Variations Working Group, to review the legal mapping performed by staff from Sturgill Turner Barker Moloney and determine the major legal issues uncovered through this process.

CHFS submitted an Interim Variations Report to RTI in November 2006 and supplied the raw data collected through the Variations process to the project site of the national Health IT Web Portal operated by the Agency for Healthcare Research and Quality.

In the months following submission of the report, staff also conducted interviews with public health officials and mental health and substance abuse stakeholders to ensure that the business practices collected were complete and accurate. The project team also convened a stakeholder feedback meeting to analyze the initial findings from the interim reports during the Kentucky e-Health Summit in January 2007

- **Solutions Identification and Analysis Process**

Following completion of the Interim Variations Report, UK and Cabinet staff provided a detailed briefing for the Solutions Working Group (SWG) members in early November 2006. Many of the group had also participated in the initial project retreat in August 2006. While many of the participants did not believe they had the answers to the thorny challenges identified by the Variations assessment process, they examined the variations identified as barriers and discussed particular approaches to dealing with these issues.

University of Kentucky (UK) faculty members, the primary project managers for this portion of the project, convened three conference calls in November and December 2006 for SWG members to discuss approaches to the barriers and aids identified by the

Variations Working Group (VWG).[1] The first conference call oriented participants to the project and the previous groups' work. In subsequent conference calls, UK staff circulated a draft of the Solutions Report with potential solutions corresponding to the barriers that the VWG had identified and asked for comments as well as assistance in identifying alternative approaches.

On January 16, CHFS submitted an interim Solutions Report Draft to RTI. On January 19, 2007, during the stakeholder discussion at the e-Health Summit, participants provided further evaluation of the inventory of solutions prepared by UK and the Solutions Working Group. From the feedback provided to the project leaders from this meeting, the Cabinet and its partners pursued further collaboration with the working groups and the Steering Committee, refined the reports, and prepared a draft implementation plan.

Because of the technical nature of the issues being assessed in the Solutions process, following the submission of the Interim Solutions Report, the Cabinet for Health and Family Services turned to the Steering Committee to provide its feedback on tailoring the project information gathered to date to suit Kentucky's needs, assessing the feasibility of various proposed solutions and determining the highest priority issues related to the secure and confidential exchange of health information, and assisting with further development of the Statewide Implementation Plan.

The Steering Committee met via conference call five times from January through April 2007. Three members of the Kentucky Privacy and Security project team also attended the March 5-6 national meeting in Bethesda, Maryland and gathered additional best practices from other states for consideration by the Steering Committee.

Thus, the solutions proposed in this report came from a variety of sources including:

- Background research performed by UK staff prior to the group meeting
- Web conferences hosted by RTI which were useful for identifying other areas for examination by the Solutions Working Group
- The Solutions Working Group members themselves during the conference calls
- Business practices identified as aids by the Variations Working Group
- The January 19 stakeholder feedback session
- The March 5-6 national meeting presentations
- Feedback from AHRQ/RTI review of the interim report
- Review of other states' reports.

[1] Kentucky project staff specifically kept the labels of aid, barrier and neutral because it was felt that identifying business practices where applicable as an aid would assist the Solutions Working Group with developing a list of best practices and possible approaches to dealing with challenging areas of health information exchange.

Review and assessment of feasibility and prioritization of recommendations in the Implementation Plan is based in part on the following decision matrix, developed for the Kentucky E-Health Board.

Solutions Assessment Criteria

CRITERIA	DESCRIPTION
Financial Considerations -	
• **Cost**	• Actual direct costs for a project - including acquisition of technology tools, staffing and administration, training and implementation, ongoing maintenance • Opportunity cost – if pursue this option does it preclude other favored options from occurring
• **Funding**	• Potential sources for funding a specific project exist, including grants from private sector, foundation or government sources; membership or usage fees; business loans or venture capital
• **Return on Investment (ROI)**	• Short term returns – how much and to whom do returns go among stakeholders • Long term returns – how much and who benefits among stakeholders • Geographic diversity of returns – do all areas receive returns or only viable in urban or rural areas
Fit	• Meets real needs in health care among patients, providers, practitioners and payors • Builds on existing e-Health and privacy and security projects, experience and infrastructure • Matches policy and business environment
Capacity Building	• Makes incremental steps toward adoption of EHRs • Builds toward long-term goal of a fully secure, interoperable EHR
Adoption Issues	• Is easy for doctors, other health professionals and staff to implement and use • Fits with office workflow
Alignment with National Trends	• Fits with national goals, standards and projects • Aligns with national trends in pay for performance, quality reporting, value-based purchasing, cost containment, and administrative efficiency
Communication Issues	• Urgency for action • Health care stakeholders see proposal as both realistic and stimulating • Compelling story for media and general public
Risk Quotient	• Commitment to "Do no harm" • Failure to launch creates no adverse incentives • Buy-in and work plan are feasible and practical

Adapted from Connecting for Health, Markle Foundation, (2004) Financial, Legal and Organizational Approaches to Achieving Electronic Connectivity in Healthcare. Retrieved on March 29, 2007 from http://healthcare.xml.org/resources/flo_sustain_healtcare_rpt.pdf

The Steering Committee examined all of the proposed solutions identified and provided input into the feasibility and relative importance of each. None of the solutions identified during this project were deemed unacceptable to the Committee. There was discussion, however, regarding restraints due to limited resources and the need for prioritization of activities in the implementation plan.

2.3 Description of report limitations

This report stems from a federally funded project with contractual obligations to use a specific research design and data collection methods that ensured a coordinated schedule and a uniform process across all states participating. At the center of the study was the use of 18 health information exchange scenarios. All stakeholders involved in the project in Kentucky were asked to utilize these scenarios during the Assessment of Variations and Solutions process. (See Methodology section below and Appendix B for further information.)

The findings, while broad in scope, are not intended to be an all-encompassing view of Kentucky's e-Health and privacy and security issues. Much more could be said about both health information exchange and privacy and security than what is contained in this report. Thus, this report is neither a manual for health information management nor a preemption analysis of HIPAA and Kentucky state law, both of which exist already in Kentucky (see references for links to this information).

While collecting data using the scenarios was important for the sake of uniformity, project participants also frequently expressed the view that there were likely Kentucky-specific issues related to privacy and security and health information exchange that the scenarios did not address. As much as possible, project staff encouraged stakeholder participants to go "off script" to capture any practices or laws that affected health information exchange in Kentucky but were not evident from the scenarios provided. A few additional areas were identified (e.g., the personal representative issue discussed below). However, there may well be other examples like this where a significant difference between federal and state law exists that were not revealed during this project process. In addition, stakeholders found that the identification of best practices for health information privacy and security at times difficult due to the discussion being driven by the scenarios.

Another limitation to this study was the lack of consistent stakeholder participation in all stages of the study process. With a voluntary project such as this, some degree of absenteeism is expected from meeting to meeting, especially because stakeholders and their organizations are not compensated for their time. The technical nature of the subject matter as well as the complex project design meant that most stakeholders needed a few meetings to become oriented to the process in order to provide truly deliberative feedback and responses. Once stakeholders were oriented to their roles, then the working groups in which they were involved may have completed their work and the orientation process needed to start with a new group. This created some

discontinuities for project staff. Fortunately, Kentucky had a number of privacy and security experts and engaged stakeholders who helped to ensure that the data collected were sound and reflected current practice.

3.0 Assessment of Variations Findings

3.1 Observations and Issues – Variations in Business Practices

The Variations Working Group (VWG) was responsible for participating in discussions regarding the 18 scenarios provided by RTI. During the Variations Assessment process the VWG collected more than 125 organization-level business practices for exchanging health information in a confidential and secure manner, The VWG was also responsible for categorizing the business practices for further review by other project working groups for the project. An overview of the major critical observations that emerged during the discussions with the VWG follows.

(1) Issues Regarding Information Transfer

Critical observations for scenarios 1 through 4 revolve around the issue of information transfer. A critical observation for Scenario 1 was the difficulty of information transfer when the mental status of a patient is unclear. Verification of the authority of persons other than the patient to make decisions on his/her behalf, as well as verification of authority between hospitals, especially when those hospitals are in different states, highlighted some of the complexities involved. Included in Scenario 2 was the recognition that there is general misunderstanding about how information can be transferred between provider organizations. In addition, state restrictions on the transfer of patient information related to substance abuse prevented the transfer of this information between substance abuse facilities and primary care providers. Similar federal restrictions prevent mental health information from being transferred. Scenario 3 highlighted the barriers posed by software applications and systems that cannot communicate with each other. Complicated authentication procedures for providers seeking access to patient information also posed a significant barrier. Scenario 4 included the challenge of defining the minimum amount of information necessary when sensitive issues arise, as well as different types of data transfer and the difficulties that arise with secure transmission for those types of data transfer.

(2) Electronic Information Exchange Between Entities

For Scenarios 5, 6, 9 and 10 the group was congruent in its view of the practices and agreed that the business practices identified were all essentially practiced at the participant's respective entities. While there were variations in *procedures* among stakeholders, the practices for exchanging health information were not significantly different. The experience of the participants is also that most providers employ basic, reasonable practices to comply with state and federal law.

A distinction between barriers and neutral practices was observed. Neutral practices generally reflected administrative processes external to the actual functioning of an electronic health records system while barriers generally were identified with requirements that must be met within the actual EHR system. An item was deemed a barrier in this regard if the participants knew that their organization, in the present regulatory, cultural and legal environment, would not change its practice. This is an important point that must be addressed in this overall research. Regardless of any strict legal interpretation that may enable a practice to avoid classification as a barrier, if the entity believes that failing to continue the practice exposes it to an unacceptable risk of negative public relations risk, civil litigation risk, or information insecurity, the practice is likely to be continued and pose a barrier to interoperability even if the barrier is not a technical legal barrier.

A related problem is that best practice (or even good practice) in the information and data security domains is inherently at odds with the free flow and exchange of electronic information between untrusted entities. The numerous competing information systems and frequent lack of universal hard to circumvent standards that are encountered in electronic health records systems, methods of transmission, methods of establishing trust and authentication and in electronic data formatting (to name but four example areas) will significantly impede transparent inter-entity electronic health record exchange.

An equitable, workable, realistic method of incentives, combined with appropriate and carefully drafted legislation may be required to facilitate inter-entity electronic health record exchange in the near to mid-term. Employees and leadership within organizations were characterized as a group as being too busy addressing their entity's on-going health and viability to be independently motivated to expedite EHR exchange. Market dynamics and resultant incentives, by themselves, can change this but the process is usually gradual.

Finally, it is important to note that the group that should stand the most to gain from this endeavor, individual consumers, has been left out of the HISPC process. The real world needs and requirements of the health care consumer, as the empowered owner and administrator of their own health records, should be addressed.

(3) Use of Patient Data

Critical observations for Scenarios 7, 8 and 11 revolved around the intricacies of ensuring that patient data is used in legitimate and ethical ways. For Scenario 7, mechanisms such as the Institutional Review Board must in some circumstances be revisited if the data will be used in ways other than it was originally intended. Other issues included the possibility of obtaining a second authorization from the patients for the new research use(s), and de-identifying data so that responses cannot be traced back to respondents.

The primary issue for Scenarios 8, 12 and 13 was under what circumstances the hospital would release information, either to law enforcement or to parents. Participants

agreed that while the hospital would release information to law enforcement under a number of different conditions (i.e., the patient signs an authorization form, the police have a legitimate reason to request as defined by HIPAA, or they have a subpoena), information would only be released to the parents if the patient signed an authorization form.

For Scenario 11, participants agreed that while under certain circumstances patients may be given the opportunity to avoid having their medical and demographic information shared, that generally, medical information may be used by a medical center's marketing department. Critical observations included the use of health information to alert a patient about new programs or products that can be of use to the patient if the patient gives authorization to be so notified. However, the use of medical information for true marketing would be prohibited by HIPAA without obtaining the patient's permission through an authorization. The use and/or disclosure of very limited patient information for fundraising is allowed but the limitations on the amount of information that can be used or disclosed significantly restricts these types of activities. The individual's diagnosis could not be used for fundraising without obtaining permission through an authorization.

(4) Release of Patient Data

Scenarios 14, 15, 16, 17 and 18 revolved around the issue of under what circumstances a patient's data may be released. Scenario 14 addressed a work related injury, and the group concluded that the patient's information cannot be shared with the employer without obtaining the individual's permission through an authorization. If the authorization were obtained, any electronic transmission would have to be secure. Critical observations drawn from the business practices implicated by Scenario 15 showed that protocols were in place for such information to be shared as needed, and that these procedures, codified in state law, are an aid to the exchange of the information. The business practices for Scenario 16 demonstrated that there is currently a system in place for exchanging newborn screening information that is specified in state statute.

Under Kentucky and Federal law, the disclosure of drug and alcohol information requires the individual's permission in most circumstances, including payment. Thus for Scenario 17, the sharing of information with the county would only be permitted if the patient authorized it. The sharing of information other than drug and alcohol treatment information would be permitted with the family member. The homeless shelter did not appear to be a covered entity; thus, they would not have the restrictions placed on covered entities by federal law.

Critical observations for Scenario 18 were that the required contracting including a business associate agreement would be cumbersome. The university would be limited in its further use or disclosure of the information beyond the terms of the contract. Securing the information and controlling access could be an additional burden on the holder.

3.2 Overview of Observations and Issues - Legal Issues

The Variations Working Group was responsible for identifying business practices for exchanging protected health information. The Legal Working Group was responsible for analyzing the business practices that impeded the flow of health information (i.e., "barriers") and mapping those practices back to state or federal law where applicable. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provided baseline protections for health information across the United States, but other state and federal laws also contain provisions regarding the privacy and security of protected health information (PHI). In some cases business practices were found not to have any basis in law but were misinterpretations of existing law or regulation. Of particular interest to the Legal Working Group members were those practices that were based on Kentucky state law rather than HIPAA.

Building upon the previous analysis, this section provides a high-level overview of the major issues that the legal mapping performed by the Legal Working Group and attorneys from Sturgill, Turner, Barker, and Moloney uncovered during the Legal analysis portion of this project.

(1) Kentucky state regulations use inconsistent standards for sharing health information.

Experts estimate that 80-90 percent of health information exchange occurs within a local area. Given this reality, if providers in a given area or state must each abide by different rules regarding the exchange of health information then it may be difficult to utilize technology to allow efficient and appropriate use of health information exchange to improve care. Members of the legal working group cited Kentucky's own health facility licensing laws and regulations and their differing confidentiality provisions as a major barrier to the interoperability of health information.

Kentucky's medical records provisions are found largely in Kentucky Administrative Regulations (KAR) Title 902, Chapter 20, regulations governing licensing for health care facilities of various kinds, including hospitals, skilled nursing facilities, and home health agencies. In these regulations, there are multiple standards for retention, access and transfer of medical records across different types of health care facilities. In some cases, the regulations require a "proper release" to transfer records to another health care provider for the purposes of treatment. This language differs significantly from HIPAA's exception for treatment, payment and operations. Thus, regulations requiring a release are more stringent than HIPAA and therefore preempt HIPAA. While many of these regulations also emphasize the need for continuity of care, the requirement for a release before sharing information for treatment means that some health care information may not be accessible. In an electronic environment, this may also impede timely information exchange. In the case of mental health and substance abuse facilities, for instance, the more stringent requirements for transferring health

information may be an entirely appropriate protection due to the sensitivity of the kind of information.

Nevertheless, although different standards for different types of information, such as mental health or substance abuse information, is appropriate, it does not follow that different health care facility types should handle that protected health information differently. Protected health information should be guarded equally whether it is a hospital, skilled nursing facility or home health agency that is storing, receiving or sending it. Health care providers involved in this project indicated that potential problems due to differing standards are often mitigated by seeking a release from patients as they register. Even so, the many differing standards in Kentucky law and regulation create confusion among administrative staff and therefore may constitute a barrier to the appropriate exchange of health information.

Health Care Facility Licensing Regulations: Release of Information Requirements	
Provided below are lists of the regulations that do and do not require a release for exchange of information in Kentucky.	
No release needed for transfer of health records for treatment	**"Proper release" needed to disclose health information**
• 902 KAR 20:016 Section 3(6)(c) 2 &(7) • 902 KAR 20:018 Section 3(4)(b)2 • 902 KAR 20:026 Section 3 (7)(e) • 902 KAR 20:036 Section 3(6)(c) • 902 KAR 20:048 Section 3(8)(f) • 902 KAR 20:051 Section 3(8)(f) • 902 KAR 20:086 Section 3(9)(f) • 902 KAR 20:240 Section 2(8)(b) • 902 KAR 20:291 Section 3(8)(e) • 902 KAR 20:300 Section 3(5)(b)	• 902 KAR 20:058 Section 3(5)(c) • 902 KAR 20:073 Section 3(4)(c) • 902 KAR 20:074 Section 6(3)(f) • 902 KAR 20:260 Section 3(5)(c) • 902 KAR 20:275 Section 3(5)(c) • 902 KAR 20:370 Section 2(4)(c)

(2) There are widespread inconsistencies between federal and state law and regulation.

Project participants expressed their greatest concern regarding the large number of differing standards and interpretations between state and federal laws protecting health information. With regard to federal law, clearly HIPAA is the biggest issue since it created a national baseline for protecting the privacy and security of an individual's health information. HIPAA itself is a lengthy and complex law, as are its many associated regulations, including most notably the Privacy Rule and the Security Rule. While the law was intended to create baseline protections and consistency across

jurisdictions, it has also spawned an entire cottage industry of experts and attorneys needed to navigate its legal and regulatory ambiguities.

The general standard for health information exchange under HIPAA is that authorization is required in order to disclose protected health information except under certain important conditions (45 CFR § 164.508). The most common of those exceptions is the TPO exception in 45 CFR § 164.506 that allows protected health information to be disclosed without authorization for the purposes of treatment, payment and operations (TPO). Other notable exceptions where authorization to disclose PHI is not needed are for medical emergencies and for 12 national priority areas including regulatory oversight, identifying abuse or neglect, public health reporting, law enforcement, and health research, to name a few. In every situation, HIPAA urges disclosure of only the "minimum necessary" information to accomplish the purposes of the information exchange. In other words, although an entity may have volumes of information about a patient, only what is necessary to fulfill an information request or to ensure continuity of care should be disclosed.

While HIPAA may be the most central federal law guiding the exchange of protected health information, an entire alphabet soup of federal laws also govern this area. Significant federal laws include the federal laboratory laws (CLIA), federal employee benefit laws (ERISA), education records (FERPA), and federal laws relating to mental health, substance abuse, communicable diseases and sexually transmitted diseases. The different federal laws raise the question of which law or regulation applies and under what circumstances.

Adding to this complexity are the varying state laws governing health information exchange. While HIPAA created a national baseline for protecting health information, it did not override state law in a comprehensive manner. When state law provides more stringent protections for privacy and security, state laws "preempt" or override HIPAA. On the other hand, when state law and regulation does not meet HIPAA's standards, then HIPAA preempts state law. This interaction means that a preemption analysis has to be performed that compares state law and HIPAA to determine whether state or federal law governs in a given circumstance. In Kentucky, collaborative work by the HIPAA Action Workgroup of Kentucky (HAWK), the University of Kentucky and others helped to clarify state law preemptions for providers and practitioners. (More information is available at http://www.mc.uky.edu/compliance/HIPAA/HIPAAForms.htm.)

Despite attempts to provide clarity while also ensuring flexibility, the ambiguities between state and federal law cause extensive confusion and frustration on a daily basis in the health sector. Although there are advantages to allowing more stringent state privacy and security protections to stand, the unintended consequence of this approach has been to create a kind of "white noise" with regard to sharing protected health information. The complexities being what they are, confusion, misinterpretation and sometimes paralysis by health professionals was a consistent theme during discussions throughout the course of this project.

Thus, a number of issues emerged as the Legal Working Group compared federal law and regulation and Kentucky state law and regulation in their analysis of the business practices collected by the Variations Working Group and stakeholders.

(a.) Incorporation of federal law and regulation inconsistent

One way to deal with the ambiguities between federal and state law is to incorporate federal law by reference in state statute and regulation. Kentucky's legal analysis did not find this practice to be widespread in state laws and regulations governing privacy and security.

One example of state law incorporating federal standards is in 908 KAR 1:320 related to substance abuse records. This regulation incorporates CFR Title 42, Chapter 1, Part 2, 'Confidentiality of Drug and Alcohol Records', which governs the use and disclosure of the PHI in drug and alcohol treatment programs. As such, the state regulation is consistent with federal regulation and creates consistency for health care entities.

Another example in Kentucky law is found in 902 KAR 20:074, the regulations for outpatient treatment facility records. This regulation states:

> Section 6. Medical Records.
> (2) Confidentiality. Confidentiality of patient records shall be maintained at all times and in accordance with 42 U.S.C. 1320d-2, the Health Insurance Portability and Accountability Act of 1996, and applicable state and federal law.

The practice of incorporating federal law and regulation by reference is by no means widespread in Kentucky law and regulation. Moreover, although this practice may possibly clarify the legal framework for privacy and security, it does not deal with every challenge.

(b.) Lack of HIPAA TPO exception in Kentucky law and regulation

One area of significant difference in state versus federal law is the lack of a treatment, payment or operations exception in Kentucky state regulations governing medical records. Several examples of state regulation preempting HIPAA were discussed during the project. One of the most significant is 902 KAR 20:016, the regulation governing hospital medical records which states:

> 902 KAR 20:016. Hospitals; Operations and Services
> (11) Medical and other patient records.
> c) Records of patients are the property of the hospital and shall not be taken from the facility except by court order. A patient's records, or portion thereof, including x-ray film, may be routed for consultation.
> 2. Patient information shall be released only on authorization of the patient, the patient's guardian, or the executor of his estate.

This regulation is more stringent than and therefore preempts HIPAA. Thus,tthe widespread practice among hospitals and other facilities in Kentucky is to incorporate a patient authorization or release of information in the registration materials to ensure that hospitals may disclose information to insurers and others necessary for treatment, payment and operations.

Another example of lack of a TPO exception in state regulation comes from physician licensure requirements. Kentucky is one of a few states that incorporate the Principles of Medical Ethics of the American Medical Association and the American Osteopathic Association into physician licensure requirements. 201 KAR 9:005 (AMA Code of Medical Ethics, E-5.05) states, "The physician should not reveal confidential communications or information without the express consent of the patient, unless required to do so by law." 201 KAR 9:005 is more stringent than, and, therefore, preempts, HIPAA. Under this provision and in some circumstances, conceivably a physician could unlawfully disclose information that otherwise would be allowed under HIPAA. In most cases, a physician would need to include a release or authorization form that allowed disclosure of the information.

(c.) HIPAA preemption of state laws and regulations

While state law may preempt HIPAA, it is just as common, if not more so, that HIPAA's provisions preempt state law or regulations. However, those state laws may not have been updated to reflect this change and therefore may be a continuing source of confusion to health care professionals.

One such example surfaced during discussion of a scenario related to hospital fundraising. As discussed above, 902 KAR 20:016, a regulation regarding hospitals, preempted HIPAA and would allow information to be disclosed to an external entity only for "consultation." There would be no controls in state law, however, on the use of PHI internally within the hospital. Thus, state law is contrary to HIPAA section 3(11)(c)(1) concerning marketing and fundraising that provides broad authority for a hospital to "access" or use PHI for "authorized" activities without an authorization for marketing or fundraising activities. The HIPAA rule permits use/disclosure of limited PHI for fundraising but further requires the individual be given the opportunity to opt out of receiving fundraising communications. 902 KAR 20:016 would not limit hospital use of the data internally. This regulation is less stringent than the applicable HIPAA rule and is, therefore, preempted by HIPAA.

This example particularly illustrates the situation-specific nature of preemption analyses of either HIPAA and state law and the reasons for the widespread confusion among health professionals. It is simply not practicable in a health care setting to consult an attorney every time a situation like this arises where state and federal law conflict. While health care providers have managed to deal with the more common challenges that arise from the state-federal misalignment, there is an underlying concern that there may

be hidden problems that a specific situation may uncover, thus exposing health care entities to unanticipated consequences.

(3) Kentucky state law and regulation are relatively silent on electronic health information exchange

Although SB2 established the framework and impetus for a statewide e-Health network in 2005, much of Kentucky law and regulation governing health care and public health assumes and reinforces a paper-based environment. The participants in the Kentucky e-Health privacy and security project, particularly those participants that utilize clinical information systems and electronic medical records, identified a number of issues in law and regulation.

In some cases, law and regulation may simply be out-dated and have not changed in decades to reflect current practices. Updating privacy and security statutes and regulations may also be an arduous task, because applicable laws and regulation are scattered throughout state codes. In some cases, too, law has not kept pace with new developments. Emerging practices such as e-prescribing, health information exchange, RHIOs, and personal health records are so new and dynamic that health care entities are operating without clear legal parameters, despite the importance PHI privacy and security. Without clear policy guidance, health organizations may be reluctant to move aggressively into the world of e-Health. Examples of specific Kentucky state regulations that are incongruous with e-Health are provided below.

(a.) State regulations generally assume paper-based system

Participants, repeatedly stated that federal and state regulations often favor a paper-based system. In various sections of Kentucky's licensing regulations, for instance, the requirements for medical records states:

> 902 KAR 20:026. Operations and services; skilled nursing facilities
> Section 3. Administration and Operation
> (10) Medical Records.
> (a) The facility shall develop and maintain a system of records retention and filing to insure completeness and prompt location of each patient's record. The records shall be held confidential. The records shall be in ink or typed and shall be legible. Each entry shall be dated and signed.

Surveyors and regulators visiting facilities often interpret this regulation to mean that records must be in paper format and therefore require facilities to print out electronic records. However, printing out a complete electronic record may be time consuming and difficult to do because electronic record keeping does not follow the same logic as paper records.

Another example of the paper-based bias is found in 902 KAR 20:091, the regulations governing community mental health centers that states:

> (4) Client records. A client record shall be maintained for each individual receiving services.
>
> > (c) Each client record shall be kept in a locked file and treated as confidential.

Each of these regulations, if interpreted loosely, may accommodate the use of electronic records but this is by no means certain. While minor, this annoyance and lack of uniformity creates another hurdle to the adoption of electronic health records.

One example in hospital regulations explicitly recognizes the existence of electronic records as well as paper. 902 KAR 20:016, Section 4 states that, "A hospital using automated data processing may keep patient indices electronically or reproduced on paper and kept in books." Whenever regulation or statute recognizes the use of electronic health record keeping and information exchange, these laws can provide some guidance to health organizations but such references are few in Kentucky state law.

(b.) Lack of clarity on sharing data with RHIO/HIE

As e-Health has progressed, regional health information organizations (RHIO), health information exchange (HIE) organizations, and subnetwork organizations (SNO) have emerged as the vehicles for sharing electronic health information. In Kentucky state law, there is no official recognition of these types of organizations yet. While SB2 authorized the creation of a statewide e-Health network, the law does not reference local e-Health organizations or provide guidance as to how state and local efforts should work together. While silence in law about these matters does not preclude collaboration by health organizations, there are inherent risks that organizations must weigh in their decision to participate in a collaborative e-Health venture.

One example discussed during the deliberations over this project involved the ambiguities for physicians and hospitals in providing data to a RHIO. Business associate agreements would have to be forged between the RHIO and each entity sharing information with it. Also, as discussed previously, because Kentucky hospital and physician licensing regulations are currently more stringent than HIPAA concerning sharing PHI, each organization would need to incorporate the sharing of PHI with a RHIO or HIE into their patient release forms, authorizations and notice of privacy practices. While these business practices would deal with the legal issues involved in sharing data with a RHIO or HIE, participants recognized that adding these new processes could be time-consuming and costly for organizations and therefore affect their willingness to participate in a local HIE or RHIO.

(4) State laws lack consistent standards for sensitive protected health information

Another challenging area for participants was the handling of certain categories of PHI that are particularly sensitive and that may have special protections. Particularly sensitive areas include information related to mental health, substance abuse, HIV/AIDS, sexually transmitted diseases and some other communicable diseases. The consensus of participants was that in law and practice these types of sensitive PHI are afforded special protections and that this is particularly important given the stigma and potential negative consequences of inappropriate disclosure.

Examples of the special protections afforded sensitive PHI in Kentucky are found in 902 KAR 20:320 and 902 KAR 20:180 related to mental health treatment. Both of these regulations require "written consent" for disclosure of medical records and patient information, even for sharing aftercare information with another provider. These protections are consistent with federal law.

While agreeing that special protections for sensitive health information are important, participants also noted the difficulty of ensuring compliance with all the provisions found throughout state and federal law related to sensitive PHI. Statutes and regulations at both the state and federal levels regarding mental health, substance abuse, and STDs are scattered throughout codebooks and administrative regulations. The differing provisions and standards for appropriate disclosure means that, when in doubt, health organizations do not share any health information. In addition, some RHIOs and HIEs are reported to decline any sensitive PHI to avoid any issues of violating privacy. Nevertheless, this policy could affect greatly both the continuity of care and the quality of care provided as electronic health information exchange becomes the norm.

Some participants urged the development of a more coherent set of standards around sensitive PHI. Such standards could have two positive benefits: 1) ensure to a greater degree that sensitive PHI is afforded the special protections it deserves and 2) make it easier for health organizations to comply with the law. More on these recommendations is provided below in the Solution section.

.

(5) Misunderstanding exists regarding the use of transfer agreements for disclosure of patient information.

In Kentucky, many different health care facilities that do not provide a full compliment of inpatient services, such as rural hospitals and specialized treatment facilities, are required by state licensure regulations to have transfer or affiliation agreements in place. One example of this is 902 KAR 20:016, which states:

> Section 3. Administration and Operation.
>
> (7) Transfer procedures and agreements.
>
> (a) The hospital shall have a written patient transfer procedure and agreement with at least one (1) of each type of other health care facility able to provide a level of inpatient care not provided by the hospital. A facility which does not have a transfer agreement in

effect, but has documented a good faith effort to enter into such an agreement, shall be in compliance with this requirement.

During the Variations Assessment discussions, some participants stated that some health care facilities would only disclose information to facilities with which they had a transfer agreement in order to comply with state law. The Legal Working Group examined this practice and tried to map it back to state law. However, the Legal Working Group found that the provisions for transfer agreements are not intended to address the use and disclosure of PHI, but the actual physical transfer of a patient. State law does not require such transfer agreements in order to exchange PHI with other providers or health care facilities. While this practice is not widespread in Kentucky, it does illustrate the difficulty that health professionals face in deciphering the complicated relationships between state and federal law. This business practice was adopted to ensure compliance with state laws protecting health information, but it also serves as a barrier to the exchange of health information.

(6) Private providers and practitioners unclear about information disclosure related to public health emergencies

In discussing scenarios related to public health reporting and bioterrorism, it is clear that public and private entities differ with regard to sharing PHI. Particularly in times of a public health emergency, it was the understanding of public health officials that they had broad legal authority to share PHI with law enforcement, public health agencies, first responders and private health care providers when needed. Private sector health organizations expressed much less certainty about how much health information they were authorized to disclose and to whom.

At the heart of this issue, too, is the fact that consulting legal counsel in the middle of an emergency is not practical. Roles and responsibilities of both public and private providers and responders need to be clear beforehand.

HIPAA provides these rules on disclosure of PHI for public health purposes:

> 45 CFR §16.512(b)(1)(i). Authorizes covered entities to disclose PHI to public health authorities authorized by law (*e.g.*, CHFS - Department of Public Health and local health departments) to collect or receive such information for the purpose of preventing or controlling disease and injury.
>
> 45 CFR §164.512(b)(1)(iv). Authorizes covered entities to disclose PHI to persons who may have been exposed to a communicable disease or may otherwise be at risk for a disease or condition if the covered entity is authorized by law to make such a disclosure in the conduct of a public health intervention or investigation.

45 CFR §164.512(j)(1)(i). Authorizes covered entities to disclose PHI to avert a serious threat to health or public safety to a person the covered entity reasonably believes is able to prevent or lessen the threat. 45 CFR §164.512(j)(4) provides that such a disclosure is presumed to have been in good faith if the belief of the threat is based upon the covered entities actual knowledge or in reliance on a credible representation made by a person with apparent knowledge or authority.

For comparison, Kentucky state law and regulation governing disclosure for public health purposes states:

KRS 214.010. Physicians and heads of families to report diseases to local board of health.
Every physician shall report all diseases designated by regulation of the Cabinet for Health and Family Services as reportable which are under his special treatment to the local board of health of his county, and every head of a family shall report any of said diseases, when known by him to exist in his family, to the local board or to some member thereof in accordance with the regulations of the Cabinet for Health and Family Services.

KRS 212.715. Orders of Health Agencies.
No person shall fail or refuse to observe or obey a written order of any board of health, department of health officer, issued pursuant to the provisions of law or regulations adopted there under.

902 KAR 2:020. Disease surveillance.
KRS 214.010 requires every physician and every head of family to notify the local health department of the existence of diseases and conditions of public health importance, known to him or her. This administrative regulation establishes notification standards and specifies the diseases requiring urgent, priority, or routine notification, in order to facilitate rapid public health action to control diseases, and to permit an accurate assessment of the health status of the Commonwealth.

While Kentucky law and regulation make clear private providers' responsibility to report to local and state public health authorities, less clear is whether they have the authority to report the information to any other entity, such as other providers or law enforcement.

(7) Legal Representative issue in Kentucky unclear and can hamper information exchange.

Another issue that arose in project discussions was the lack of clarity in Kentucky law related to personal or legal representatives. Under the HIPAA Privacy Regulation, health organizations must treat a personal representative as just as the organization would treat the individual who is the subject of the PHI. Thus, under federal law, a personal representative has all the rights that a patient would have. In Kentucky state

law, however, a personal representative is a special category of legal representative allowed only under certain circumstances, such as:

- when a court has appointed someone as a legal guardian,
- an individual has been granted specific power of attorney to act on behalf of a patient, or
- a patient lacks “decisional capacity” and there is no legally executed document directing who should make health care decisions for the patient.

Personal representative status is granted in descending order to:

1. The judicially appointed guardian, provided that medical decisions are within the scope of the guardianship;
2. Spouse of the patient;
3. Adult child of the patient or a majority of children if the patient has more than one child;
4. Parents of a child;
5. Nearest living relative; or
6. Executor of a patient’s estate.

Moreover, the personal representative is not generally treated in the same manner as the individual patient and can only give authorization for disclosure of PHI relating to the matters for which he or she is representing the patient. Minors are also afforded special rights under Kentucky law and may seek treatment without parental consent under certain circumstances.

According to participants in this project, the additional strictures in Kentucky law related to personal representative often hamper the flow of information because there is a great degree of ambiguity and complexity to the law. Therefore, it may be unclear who may reasonably execute a release of information for an incapacitated or intellectually disabled patient. Clear guidance to health care entities concerning the use and disclosure of protected health information to legal representatives is needed.

4.0 Summary of Key Findings from the Assessment of Variation

4.1 Summary of Business Practice Variation Issues

Four overarching themes emerged as business practices for the 18 scenarios that were examined: 1) information transfer; 2) access to data; 3) de-identifying information; and 4) utility of established systems. Regarding information transfer, the issues were numerous and wide-ranging. First was the difficulty of information transfer when the

Key Issues Found in Business Practice Assessment:

- Information Transfer
- Access To Data
- De-Identifying Information
- Utility Of Established Systems.

mental status of a patient was unclear, specifically, whether the patient was lucid enough to make decisions and if not, whether a family member was legally able to make those decisions for the patient. Second was lack of clarity about how information may be transferred between provider organizations and the related issue of defining the minimum amount of information necessary when sensitive issues about a patient's medical information arose. Third were the barriers posed by technical systems that cannot communicate, and the associated problems of the various types of data transfer along with the difficulties that arise with ensuring secure transmission.

Access to data also posed a number of interrelated issues, all revolving around the question of when patient data may be released, and to whom. For medical purposes, issues arose regarding the release of information for payers to authorize payment, as well as for organizations to monitor patient management. Business practices were also examined regarding the release of information for non-medical purposes, such as to police, parents of adult children, employers, and government agencies. Finally, business practices were examined related to marketing endeavors, either by the marketing department of a medical center, or through the sale of patient data to third parties.

The issue of de-identifying information also surfaced as a major theme of the business practices. In two cases, the concern centered on monitoring patients, either for provision of preventive services or for research purposes. In the third instance, the Governor of a state requested that information be left identifiable so low-income children could be monitored to ensure they were receiving health care that was deemed necessary.

Finally, several systems already in place were examined to explore their utility and whether business practices for those systems were already in place. The systems included Communicable Disease Exposure Tracking, Interstate Public Health Data Exchange, Infant Genetic Disorder Registry and the Interactive Voice Response System.

A number of interesting observations and issues emerged from the working groups' deliberations that were not directly solicited by the scenarios. Primary among the issues discussed was the unintended consequences of HIPAA, including a general lack of awareness of the law and frequent misunderstandings that arise as to whether HIPAA allows a certain kind of activity or not and under what circumstances.

The second observation/issue was the lack of a scenario or information domain provided that dealt with laws, regulations and policies affecting the exchange of protected health information (PHI) through an exchange mechanism controlled by the consumer or patient of their information. For example, PHI exchanges directly between entities (e.g., drug abuse treatment center to a family physician) are carried out under a set of state and federal laws and regulations combined with local business practices. These restrictions generally limit which data can be shared about individuals under a variety of circumstances.

With the growing number of vendors, health plans and employers that are offering personal health records and the growing number of RHIOs and states examining health record banking, consumer-controlled electronic exchange is becoming a realistic possibility. If a data exchange was under the control of the subject of the data, the patient about whom the drug abuse treatment center and the physician were exchanging data, the entity providing the information is effectively providing it to the patient along with a request to send the data on to the intended physician recipient. The recipient of the data is getting it from the patient (including the digital signature of the original source of the data). Of course, as a routine matter exchanges would be vetted by a software agent of the person (i.e., the data subject) that had been configured by that person to allow (and log) data exchanges he/she considers permissible. All other attempted exchanges would be returned to the originator (with a log of the event available to the patient).

From a legal point of view this subject-controlled exchange is similar to what happens today when a patient takes his/her physical records from one provider to another. In this case, the health provider gives a copy of the records to the patient with the knowledge that no law prevents this. In the vast majority of cases, the law requires that the patient be provided a copy of her / his records. HIPAA, for example, requires that patients be provided a copy of their records on request. So, one would expect the vast majority of data exchanges to be minimally unfettered and supported by existing privacy laws or practices if controlled by the consumer.

The third issue identified was the lack of a standard way to match patient records not only within healthcare organizations but also across healthcare organizations in a community. Patients have different medical record numbers not only within a healthcare organization but also across healthcare organizations in a community. There is no standard way to match records since the adoption of a unique national patient identifier for healthcare is not likely. Other approaches such as mapping multiple identifiers across multiple organizations vis-à-vis a master patient index are being pursued, including in Kentucky. Technologists generally see tremendous difficulties ahead without a national unique identifier for all individuals or at least a master patient index that maps to all the unique identifiers that are used for patients across the community or region. Until there is a standard way to match records this will continue to be a challenge and obstacle to developing health information exchange.

The fourth observation/issue is the inability to segregate sensitive PHI within a patient's clinical record or PHI from administrative information. Role-based access has limitations and there is a lack of standards regarding authentication, authorization, access, auditing and encryption. Since there are no standard or accepted methods, the technologic approaches across the community are various and limited.

Last of the considerations is that a health information network is only as secure as the exchange partner with the weakest security protections. A partner with poor security technology and business practices becomes a portal for access by unauthorized users. Because organizations involved with health information exchange are providing

information, there is concern about their liability with respect to the health information exchange organization in general.

4.2 Summary of Legal Issues

Fragmentation in the U.S health care system makes continuity of care a particularly serious problem. There are frequent gaps in information among organizations providing care. One goal of e-Health is to improve the efficiency and effectiveness of the care process by allowing a full and appropriate complement of health information to be available instantaneously at the point of care when needed. For instance, a patient seeking care in an emergency department generally does not have a complete medical record at hand. This is the type of situation in which being able to access a patient's medical information electronically could significantly improve care.

However, the problem is ensuring appropriate controls around protected health information. For instance, a person with a mental illness may feel it is entirely appropriate for a treatment facility to share health information with a physician providing aftercare but may not want that information shared with an employer. The Health Insurance Portability and Accountability Act of 1996 provided baseline protections for health information across the United States. Other state and federal laws also contain provisions regarding the privacy and security of protected health information (PHI). However, there are still many ambiguities in the exchange of information in everyday practice due to the complexity of HIPAA and the size and scope of its subsequent regulations as well as its overlap with other state and federal laws. Some privacy advocates believe that stronger protections are needed.

Key Issues Found in Legal Mapping & Assessment:

- Misunderstanding of HIPAA and confusion of state and federal laws
- Relative silence in law on health information exchange
- Lack of uniformity regarding handling of sensitive PHI
- Concern Regarding Adverse Legal Action
- Public Perception and Business Risk Related to Confidentiality of PHI

Participants in the Kentucky e-Health Privacy and Security Project echoed a concern that is widespread in the e-Health world. For technology to improve efficiency and quality of health care to the greatest degree possible, health information exchange must be automatic, and this is largely based on the use of a set of recognized standards among organizations, including privacy and security standards. Thus, state or federal laws and regulations that represent significant deviation from the baseline privacy and security protections that HIPAA provides can be particularly problematic in an electronic information environment.

Health information technology vendors develop electronic health record software and other applications in compliance with national standards and may not recognize the state-specific variations with regard to privacy and security practice. For example, the federal HIPAA statute and regulations authorize the sharing of PHI among entities without a patient's authorization if the disclosure is done for the purpose of treatment, payment or operations. However, a given state's laws may have more stringent privacy protections and allow PHI to be forwarded without authorization only for treatment purposes but not for payment or operations. In another state PHI may be forwarded for operational purposes within an organization but not for any reason to other entities without first seeking an authorization for release of the information. Health IT vendors in these situations where state law preempts HIPAA may then have to make costly changes to their software to deal with the specific issues in state law, or providers in that state may need to develop costly manual procedures to ensure their systems are compliant with state laws.

The current climate of widespread misunderstanding and confusion around HIPAA and its preemption of state law are not conducive to the development of electronic health information exchange. Kentucky stakeholders agreed that clear, consensus-based standards for when health information exchange is appropriate and need to be in place to facilitate the growth of e-Health. As a smooth, wide road with clear markings allows a driver to go faster safely, so clear rules about when health information exchange is appropriate can enable greater efficiency in the health care system. Each state must understand the laws and regulations that guide the management of health information to determine if there are any significant legal barriers that create confusion or hinder the use of technology. In addition, clear policies for the exchange of sensitive or privileged PHI also need to be in place as well. Without these standards, the dominant concerns will be fear of inadvertent or inappropriate release of PHI, concerns regarding adverse legal action, and the impact such a release could have on a health organization's reputation in the community.

5.0 Overview of Solutions Identification and Assessment

Project staff and the Solutions Working Group members focused their attention primarily on barriers identified and analyzed by the Variations and Legal groups that were mapped back to Kentucky state law or regulation. Because the number of barriers that have their roots in Kentucky state law or regulation is relatively small, additional analyses have been performed for to the submission of the Final Solutions Report to fill in gaps to examine alternatives for dealing with barriers that have their source in federal law or it misinterpretation.

The solutions framework described in the methodology of this report evolved from the analysis of the barriers identified by the VWG and LWG during the assessment of variations process. The framework served as a means of readily identifying solutions with a similar intent and focal point, so that duplicate solutions can be eliminated and similar solutions may be consolidated as the implementation plans are devised.

There were five main categories of solutions identified and each area addresses a core area of concern identified in the variations process:

Statutory Action: The solutions in this category involve reviewing, revising, or amending state or federal laws that affect the exchange of health information, the privacy and security of health information, and the related healthcare diagnosis and treatment activity. The solutions in this category address a number of barriers to health information exchange (HIE) identified during this project including :

- Inconsistent federal law
- Inconsistent state law
- Misinterpretation or understanding of HIPAA law.

Regulatory Action: The solutions in this category identify areas where existing rules and regulations may be relaxed, modified, expanded, or better explained to facilitate HIE without the need for legislative action. These solutions address the following barriers to HIE:

- Differences in state and federal regulation
- Lack of clarity regarding state and federal regulation
- Fear of violating a regulation and subsequent sanctions or litigation.

Administrative/Organizational Action: The solutions in this category address the need to amend, create, and standardize administrative actions, business policies and practices utilized by health care providers at the individual and institutional level resulting from the following barriers:

- Longstanding cultural trends and norms within an organization
- Differences in organizational policies and practices.

Technological Solutions: The solutions in this category identify ways in which technology can be used as a solution to the barriers posed by HIE. How can health information technology improve the secure transmission of health information? What technological tools, skills or training may address the barriers to HIE? These solutions target the following barriers:

- Complexity of digital or electronic communication
- Insufficient use of electronic health information.

Public Awareness and Education: The solutions in this category address the need for increased public awareness through training and education of consumers, health care providers, government officials, professional associations, employers, public officials, researchers, and educators about the rules governing HIE, the benefits to electronic HIE, and their respective rights and obligations regarding enhanced quality of care. These solutions address the barrier of:

- Limited or lack of education about HIE and privacy and security laws
- Provider concern about business reputation and public relations issues

5.1 Legislative Solutions

5.1.1 Review, and where necessary, revise definitions related to health information sharing and exchange that presently exist in statute to make them consistent with the present meaning in a paper and electronic environment.

General context: Review laws to determine whether the meanings of terms are consistent with the capabilities that emerge for HIE in an electronic environment. Ensure that the definitions are consistently applied from one section to the next.
Privacy & security domain addressed: State law restrictions.
Types of HIE addressed: All types.
Stakeholders primarily affected: All types.
HIE barrier(s) addressed: Inconsistent state laws.
Stage of development: Conceptual.
Extent to which solution is in use: Words are frequently defined in statute and rule. Need to ensure consistency with existing rules and statutes.
Applicability of solution: Might be developed in reference to model state law.
Extent of barriers or opposition: Some terms have more than one meaning. Many terms in question have already been defined in rule or statute and may have conflicting meanings.

5.1.2 Recommend ways to reconcile differences between state and federal laws relating to preemption and interpretation, including identification and management of sensitive health information.

General context: Preemption generally refers to the displacement of conflicting or inconsistent state laws by federal laws. HIPAA is only preempted by state law that is more stringent or relates to a very narrow range of circumstances. However, the determination that a state law is more stringent must be made on a case-by-case basis and varies among analysts and practitioners. Examples of more stringent Kentucky law identified by the Legal Working Group include:

a. Absence of a state equivalent to the HIPAA treatment/payment/operations (TPO) exemption;
b. Requirement that paper documentation be produced for licensure review;
c. Lack of authorization for digital signatures; and
d. Absence of provisions expediting essential information transfer in emergencies.

Privacy & security domain addressed: State law restrictions.
Types of HIE addressed: All.
Stakeholders primarily affected: All.
HIE barrier(s) addressed: Differences in state and federal laws.
Stage of development: Conceptual.
Extent to which solution is in use: Some preemption analyses have been conducted and are available for reference.

Applicability of solution: May be some applicability across stakeholders although each issue may have unique features to be resolved.
Extent of barriers or opposition: 1) Reluctance on the part of legislators to revisit existing legislation; 2) Competing legislative priorities.

5.1.3 Consider consolidating statutes related to the exchange of health information to resolve conflicts among Kentucky laws and between Kentucky laws and HIPAA.

General context: Several chapters of the Kentucky Revised Statutes govern the way in which protected health information (PHI) may be shared. In the absence of a statutorily defined uniform patient authorization, many providers are unclear about the specific state provisions that govern the sharing of PHI that are more restrictive than the HIPAA provisions.
Privacy & security domain addressed: State law restrictions.
Types of HIE addressed: All types.
Stakeholders primarily affected: Health care providers.
HIE barrier(s) addressed: Inconsistent state laws.
Stage of development: Early stage of planning; previous proposals limited.
Extent to which solution is in use: Under discussion
Applicability of solution: Broad
Extent of barriers or opposition: 1) Reluctance on the part of legislators to revisit existing legislation; 2) Competing legislative priorities; 3) Possible opposition to specific changes.

5.2 Regulatory Solutions

5.2.1 Establish the Privacy and Security Committee of the Kentucky e-Health Network Board and charge it with providing clarification on existing regulations and creating regulations that will advance HIE.

General context: Create a statewide structure to encourage and facilitate the adoption of electronic health information exchange and to address the barriers created by public regulations and/or private policies.
Privacy & security domain addressed: All.
Types of HIE addressed: All types.
Stakeholders primarily affected: All types – focus on health care providers.
HIE barrier(s) addressed: Limited or lack of education about health information exchange.
Stage of development: Developmental: a Privacy and Security Committee has been proposed under the auspices of the e-Health Board
Extent to which solution is in use: Task force approach is frequently used to guide and direct the implementation of changes in rules and regulations. There are organizations in place with the same or similar mission (e.g. Workgroup for Electronic Data Interchange (WEDI)).
Applicability of solution: Applicable to other states and organizations.
Extent of barriers or opposition: Competition for scarce resources (time and dollars) for the establishment of another state level task force.

5.2.2 Develop a policy framework for consistent identity verification and management system of both providers and patients that request and transmit PHI.

General context: Define the criteria required to verify the identity of providers participating in an HIE. Different institutions have different processes and policies related to the verification of providers who are seeking or receiving health information on behalf of the patient.

Privacy & security domain addressed: User and entity authentication.

Types of HIE addressed: Clinical.

Stakeholders primarily affected: Health care providers.

HIE barrier(s) addressed: Complexity of digital or electronic communication.

Stage of development: Developmental.

Extent to which solution is in use: Health care providers currently use a variety of approaches to verify identity such as caller ID, use of letterhead, or call backs/fax backs to organization for a separate verification of identify.

Applicability of solution: Applicable to all stakeholders.

Extent of barriers or opposition: Cost and complexity of developing and implementing organization and technical systems that prevent identity fraud while allowing legitimate users to gain ready access to HIE.

5.2.3 Develop policies that address sharing of patient health information among private and public sector providers within and among states during an emergency.

General context: Authorize providers to obtain clinical information from other providers in the case of a disaster or other emergency where the patient is displaced and may or may not have executed authorization for HIE.

Privacy & security domain addressed: User and entity authentication, information authorization and access control, state law restrictions.

Types of HIE addressed: Clinical.

Stakeholders primarily affected: Health care providers.

HIE barrier(s) addressed: Fear of violating rules, litigation.

Stage of development: Conceptual

Extent to which solution is in use: During Hurricane Katrina, HHS Secretary suspended impediments. There is a need for an established plan or rule that authorizes exchange of information.

Applicability of solution: Applicable to all providers.

Extent of barriers or opposition: Need to explore the limitations on emergency triage protocols imposed by the EMTALA laws

5.2.4 Establish an interstate task force to develop HIE policies for the exchange of information between states.

General context: When a patient's records need to be transferred between providers in different states, each provider is subject to the laws regulating medical records in the state in which they reside/practice. An interstate task force would allow Kentucky and its neighboring states to establish guidelines for the

private and secure exchange of PHI. One useful model may be the agreements between the Kentucky Hospital Association and its counterparts in other states for the exchange of hospitalization data.
Privacy & security domain addressed: State law restrictions
Types of HIE addressed: Clinical.
Stakeholders primarily affected: Health care providers.
HIE barrier(s) addressed: Multi-state law restrictions.
Stage of development: Early stage; a proposal. **Extent to which solution is in use:** Generally ad hoc.
Applicability of solution: All participating states.
Extent of barriers or opposition: Access to adequate administrative, legal, and financial resources to implement and sustain task force.

5.3 Organizational/Administrative Solutions

5.3.1 Produce and distribute checklists, inventories of successful practices, templates, and other resources required for the establishment of a secure HIE system.

General context: Develop and distribute documents for stakeholders use to facilitate the exchange of health information, to encourage a development of a statewide HIE system, and to legitimate the request of RHIOs seeking this information from provider organizations.
Privacy & security domain addressed: Information use and disclosure policies.
Types of HIE addressed: All.
Stakeholders primarily affected: All.
HIE barrier(s) addressed: Differences in organizational policies and practices; longstanding cultural trends and norms.
Stage of development: Planning.
Extent to which solution is in use: Many organizations already distribute model contracts for their members and stakeholders.
Applicability of solution: Applicable across a variety of organizations and stakeholders.
Extent of barriers or opposition: Some resources would be required to organize and distribute information. A more significant barrier may be the extent to which organizations are willing to change their current practices.

5.3.2 Provide technical support for RHIO/HIE initiatives to identify financial resources and develop sustainable business models.

General context: RHIO/HIE initiatives typically require dedicated resources and staff to succeed, and thus must be grounded in a sound business case as well as a sustainable business model. Technical assistance from experts in the field may be available through the networking capacity of the state's e-Health Board.
Privacy & security domain addressed: Information transmission and exchange protocols.
Types of HIE addressed: All.

Stakeholders primarily affected: All.
HIE barrier(s) addressed: Insufficient adoption and utilization of electronic health information systems.
Stage of development: Planning.
Extent to which solution is in use: There are sources of grant funding – state, federal and private.
Applicability of solution: Applicable across RHIOs.
Extent of barriers or opposition: There is a great deal of competition for a limited amount of funding.

5.4 Technological solutions

5.4.1 Convene a second Kentucky e-Health Summit to share technological methodologies that will address the barriers to HIE.

General context: Bring technology providers and users together to discuss and develop new models for HIE activity and recommendations that will advance the utilization of interoperable HIE systems**.**
Privacy & security domain addressed: All.
Types of HIE addressed: All.
Stakeholders primarily affected: All.
HIE barrier(s) addressed: Complexity of digital or electronic communication.
Stage of development: Under discussion
Extent to which solution is in use: E-Health Board has used diverse strategies to develop and implement a strategy for the adoption and use of electronic health records and promote the development and implementation of a Kentucky health information infrastructure.
Applicability of solution: Kentucky's example could be followed by other states.
Extent of barriers or opposition: Competing priorities, complexity of the healthcare industry.

5.4.2 Facilitate the development of a statewide electronic health network.

General context: In order to develop a business case and momentum for statewide e-Health implementation pursuant to the legislative mandate in Senate Bill 2, Kentucky has chosen to make immediate use of existing resources; the Kentucky Health Information Partnership (K-HIP) will serve as a statewide HIE pilot that will develop a web portal to access claims-based patient health information and process administration transactions. K-HIP will also assist with the development of the basic infrastructure for HIE. Kentucky may also want to explore the feasibility and cost-effectiveness of developing a dedicated health information exchange network possibly in conjunction with other states to provide the highest level of security.
Privacy & security domain addressed: All.
Types of HIE addressed: All types of HIE can be addressed but the demand for clinical data is most critical.
Stakeholders primarily affected: Health care providers, plans and third-party payers, state government.

HIE barrier(s) addressed: All
Stage of development: Model developed for statewide web portal with patient health summary derived from electronic claims data as important preliminary step to full electronic exchange of clinical information. Assessment of cost-effectiveness, however, remains conceptual.
Extent to which solution is in use: Medicaid Transformation Grant will support initial web portal development and deployment by Fall 2007.
Applicability of solution: Solution is applicable to all states should it prove cost-effective.
Extent of barriers or opposition: Requires development of inter-organizational relationships and trust to discern necessity and sustainability as it relates to justification of barriers and expense of implementation.

5.4.3 Utilize the expertise of the Privacy and Security Committee members to develop and advise on best-in-class security and privacy solutions and technologies, such as the use of digital signatures, automated proactive audit mechanisms, and identity management for use in the HIE environment.
General context: Identify experts that could work to develop technology that supports the development of a private and secure HIE network or system.
Privacy & security domain addressed: All domains.
Types of HIE addressed: All.
Stakeholders primarily affected: All. IT Vendors, CIOs, and privacy and security officers.
HIE barrier(s) addressed: The complexity of digital or electronic communication.
Stage of development: Work in conjunction with the newly awarded Medicaid transformation grant from CMS. Groundwork in place for implementation of privacy and security plan regarding electronic signatures, for which the American Bar Association provides guidelines for use of such signatures. Federal law - Electronic Signatures in Global and International Commerce Act. Proactive audit mechanisms implemented under HIPAA Security Rule that requires covered entities to implement procedures to regularly review records of information system activity including audit logs, access reports, and security incident tracking reports ((§164.308(a)(1)(ii)(D)).
Extent to which solution is in use: The e-Health Board has drawn on the talents of many volunteers, including those engaged for the Privacy and Security Committee. Proactive audit mechanisms readily used.
Applicability of solution: All states and stakeholders.
Extent of barriers or opposition: Funding and other incentives are necessary to retain talent to implement and sustain technological required for security of HIE, such as analyzing complex and voluminous data. Barriers to adoption of electronic signatures include technical, representational, and privacy issues as well as business, cultural and usage barriers to implementation.

5.4.4 Use financial incentives and other means to encourage providers to invest in HIT and implementation of private and secure HIE methodologies and systems.

General context: There are few financial incentives related to the adoption of electronic HIE systems, in addition to the fact that utilization of electronic health records by providers is limited. Financial assistance in the development and implementation stages could provide the necessary momentum needed to create a viable network.

Privacy & security domain addressed: Information transmission and exchange protocols.

Types of HIE addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Complexity of digital or electronic communication.

Stage of development: Conceptual.

Extent to which solution is in use: e-Prescribing grants recently distributed; other grants and incentive options under consideration.

Applicability of solution: Applicable to other states.

Extent of barriers or opposition: Limited or lack of education about electronic HIE, the complexity of the industry; limited examples of financial sustainability plans that work; and competing legislative priorities if new types of tax incentives are proposed.

5.5 Public Awareness and Education

5.5.1 Prepare and distribute information resources that clarify and address the inconsistent interpretation of relevant state law and HIPAA, including the definition of health information exchange related terms in the paper or electronic environment, to educate healthcare providers.

General context: One of the findings of Kentucky's Variations Working Group was that many providers misinterpret relevant aspects of state law as well as the HIPAA Rules and Standards. Frequently they have an overly restrictive interpretation of what the rules and regulations require and in turn restrict the flow of patient information between stakeholders and to parties such as personal representatives.

Privacy & security domain addressed: State law restrictions.

Types of HIE addressed: All.

Stakeholders primarily affected: All.

HIE barrier(s) addressed: Limited or lack of education about HIE and privacy and security laws.

Stage of development: Implementation.

Extent to which solution is in use: There are a variety of organizations working to educate stakeholders on HIPAA, including health care professional organizations, the Centers for Medicare and Medicaid Services, the Office for Civil Rights and the Workgroup for Electronic Data Interchange.

Applicability of solution: Applicable to all states.

Extent of barriers or opposition: Competing priorities, employee turnover.

5.5.2 Educate patients and consumers on methods to access and manage their health information

General context: Many patients are unaware of their rights under HIPAA or of the role that e-Health can play in helping them to manage their health and health care. It is important to educate patients on how to access and manage their health information and the technological tools that are available to assist them.
Privacy & security domain addressed: Information use and disclosure policies in plain English and accessible to non-English speakers, preferably in a literally translated form.
Types of HIE addressed: Clinical.
Stakeholders primarily affected: Health care providers and patients.
HIE barrier(s) addressed: Longstanding cultural trends and norms.
Stage of development: Isolated implementation; inconsistent.
Extent to which solution is in use: Both opt in and opt out are in use.
Applicability of solution: All states.
Extent of barriers or opposition: Competing priorities, health literacy, consumer awareness.

5.5.3 Develop and implement public awareness and educational activities that provide accurate information in language accessible to the non-specialist, i.e. layman's terms, about electronic health records, rules governing disclosure of patient data, risks associated with paper charts, and the positive aspects of electronic health information.

General context: The Variations Working Group and participants in the stakeholder feedback session noted serious concerns in the area of institutional reputation and public relations. These issues could be addressed in part by creating a communication plan that utilizes a variety of channels to deliver the message that information technology and HIE improve the quality of service in the healthcare industry and should therefore be encouraged.
Privacy & security domain addressed: Could address all.
Types of HIE addressed: Clinical.
Stakeholders primarily affected: All, including the general public.
HIE barrier(s) addressed: Longstanding cultural trends and norms**,** limited or lack of education about HIE and privacy and security laws.
Stage of development: Proposal
Extent to which solution is in use: There are a variety of messages in both the professional and popular media extolling the virtues of electronic HIE.
Applicability of solution: Applicable to all stakeholders.
Extent of barriers or opposition: Need adequate funding to be effective.

5.5.4 Inform stakeholders (possibly as part of Second Annual e-Health Summit) of national, state and local activities in the area of HIT and HIE

General context: Organizing focus groups, presentations or information sessions within a political or social group or association can serve as a vehicle

for educating and informing the public of issues related to HIE. It can foster buy-in and motivate key stakeholders to support HIE initiatives.
Privacy & security domain addressed: Could address information use and disclosure policies or other issues to advance HIE.
Types of HIE addressed: All.
Stakeholders primarily affected: All.
HIE barrier(s) addressed: Limited or lack of education about HIE and limited or lack of use of electronic health information.
Stage of development: Conceptual.
Extent to which solution is in use: Used in other venues.
Applicability of solution: Applicable to other states.
Extent of barriers or opposition: Requires trained facilitators; influential stakeholders might not be available for time-consuming process, and findings cannot be generalized unless balanced representation of all viewpoints achieved.

5.5.5 Encourage the use of existing mechanisms for authorizing family members' and others' access to another's PHI, such as the durable power of attorney, health care surrogate, and living wills. Ensure that these documents authorize access to PHI in keeping with patient wishes. Identify any gaps in existing state law regarding personal representatives and others who navigate the health care system on behalf of vulnerable individuals.
Long term care providers consistently document powers of attorney for their patients. Other health care providers are less consistent in such documentation. Personal representatives for individuals with a variety of special needs report uncertainty in the provider community regarding their access to documents in emergencies or when authorization documentation is unavailable.
Privacy & security domain addressed: State law restrictions; information authorization
Types of HIE addressed: Clinical information.
Stakeholders primarily affected: Health care providers.
HIE barrier(s) addressed: Inconsistent state and federal laws.
Stage of development: Conceptual stage.
Extent to which solution is in use: Kentucky Statutes provide for a health care surrogate (KRS 311.629: Powers of Health Care Surrogate).
Applicability of solution: Broad
Extent of barriers or opposition: Funding, competing priorities, and consumer

5.5.6 Integrate and link state e-Health information with existing web sites to provide updates on state activities.
General context: Transparency initiative and state e-Health Web site can be used to carry the message of the value of electronic HIE to a wider audience and it can be used to communicate project and program progress. Limited or lacking education about HIE and limited or lacking use of electronic health information.
Privacy & security domain addressed: All.
Types of HIE addressed: All.

Stakeholders primarily affected: All.
HIE barrier(s) addressed: Limited or lacking education about HIE and privacy and security laws.
Stage of development: Implemented.
Extent to which solution is in use: The E-Health Board website includes a page on the Kentucky Privacy and Security Project.
Applicability of solution: Applicable to all stakeholders.
Extent of barriers or opposition: Cost (albeit relatively low) of hosting a web site and developing and maintaining content.

6.0 Summary of State Proposed Solutions

Statutory solutions would require the review, revision, or amendment of state or federal laws that are inconsistent with related provisions in state or federal law, threaten the feasibility of HIE, or are subject to widespread uncertainty and misinterpretation.

Regulatory solutions identify areas where regulations may be modified or clarified to facilitate HIE, including confusion or conflict between state and federal regulation and ambiguities that lead to fear of violating a regulation, with associated sanctions or litigation.

Administrative or organizational solutions address the need to amend, create, and standardize health care providers' administrative actions, business policies and practices that arise because of organizational custom and variation in organizational policies and practices.

Technological solutions to HIE barriers seek to improve the secure transmission of health information, improve professional competence regarding the nature and use of digital or electronic communication, and increase the adoption of HIT.

Public awareness and education solutions promote training and education of consumers, health care providers, government officials, professional associations, employers, public officials, researchers, and educators about the rules governing HIE, the benefits to electronic HIE, and their respective rights and obligations regarding enhanced quality of care. These solutions address the low level of education about HIE and privacy and security laws as well as provider concern about business reputation and public relations issues.

7.0 Interstate Health Information Exchange and National-level Recommendations

With regard to interstate and nationwide health information exchange, deliberations by Kentucky stakeholders revealed several areas of concern that lie beyond the authority of state government agencies or private sector organizations in Kentucky to address. The first major area of concern that must be addressed at the federal level is the issue of policy related to sensitive health information. Many health conditions such as mental health, substance abuse and sexually transmitted diseases require special protections for PHI. However, complete medical information is also critical for individuals with sensitive conditions in order to ensure quality care. Stakeholders suggested that additional clarification from the federal Office of Civil Rights at the Department for Health and Human Services related to the appropriated balance between the privacy of sensitive protected health information and right for timely and equitable quality of care could provide greater clarity regarding exchanging this kind of health information. This is particularly necessary because federal law was seen as setting the standard for health information exchange in this area.

Another issue that emerged as the vagueness of HIPAA's protections for psychotherapy notes. Although psychotherapy notes are defined in 42 CFR § 164.501, stakeholders agreed that more clarity on this portion of HIPAA would relieve providers' concerns and help ensure that the minimum necessary information is indeed shared when appropriate. Because the lack of clarity in HIPAA is the issue, then stakeholders agreed this should be addressed through federal government action.

Finally, in discussions about the move to fully interoperable electronic/personal health records, stakeholders also expressed the need for clarity on a national level on what kinds and how much clinical information should be shared. Even if a region had the capacity to share electronic health records in their entirety, most stakeholders believed that a summary of the clinical information available with the ability to seek more complete information when needed would be more helpful in a health information exchange. Thus, stakeholders stated that some form of authoritative and consistent standards for what information should be included in an electronically exchanged health record or record summary, such as the Continuity of Care Record being developed currently, would greatly facilitate interoperability and provide additional guidance for state and local health information exchange efforts.

8.0 Conclusions and Next Steps

e-Health is viewed as one of the most promising methods for addressing issues of rising health care costs, variable quality of care and poor health outcomes. In the same way that technology has transformed the productivity and efficiency of other American industries, thought leaders and innovators are looking to do the same in the $2.1 trillion health sector.

The ability to maintain the privacy and security of an individual's health information across multiple organizations is fundamental to the success of electronic health information exchange. The breadth and scope of the Kentucky e-Health Privacy and Security Collaboration demonstrated that privacy and security are fundamental to the work of the Kentucky e-Health Network Board and its efforts to foster a secure, statewide e-Health network.

Many stakeholders who participated in the deliberations for this project have agreed to continue their involvement by serving on the Privacy and Security Committee of the e-Health Network Board. The first task of this new committee will be to implement the recommendations from this report and the final Implementation Plan.

An important theme that emerged from the discussions with all stakeholder groups is that the move to electronic health information does not need to come at the expense of personal privacy and security. In fact, with appropriate coordination of policy and practice among all stakeholders, electronic health information may be more secure and better able to protect confidentiality than the current paper environment. With this as one of its goals, the Privacy and Security Committee will continue the work of the Kentucky e-Health Privacy and Security Collaboration in facilitating secure, confidential, interoperable health information exchange.

Appendix A: Steering Committee & Working Group Members for the Kentucky E-Health Privacy and Security Collaboration

1. Steering Committee

Chairs:

- Bob Esterhay, University of Louisville
- Carol Steltenkamp, University of Kentucky

Members:

- Jeanne Reiners, Corporate IT Manager, Baptist Healthcare System and the Chair of the Variations Working Group
- Vickie Yates Brown, J.D., Member at Greenebaum, Doll & MacDonald and Chair of the Legal Working Group
- Jeff Rose, Director of Technology Solutions at ConnectKentucky and Chair of the Solutions Working Group
- Shawn Crouch, Chief Of Staff, Kentucky Cabinet for Health and Family Services (CHFS)
- Trudi Matthews, Senior Policy Advisor, CHFS Office of the Secretary
- Dr. Brent Wright, Program Director, U of L Family Practice Residency Program, TJ Samson Family Practice Center
- Terry Jackson, Director of Information Services, Trover Foundation
- Joni Lemke, Program Director, Wellpoint/Anthem Privacy and Security Office
- Shannon Pratt, Government Relations Director, American Cancer Society
- Marti Arvin, Privacy Officer, Univ. of Louisville

2. Variations Working Group

Chair: Jeanne Reiners, Corporate IT Manager, Baptist Healthcare Systems

Members:

- Brenda Beckham, Director Health Information Management, Baptist Hospital East
- Jolene Eicher, Practice Administrator, Commonwealth Ear Nose and Throat
- Craig Gillespie, Practice Administrator, Pediatric and Adolescent Associates
- Bruce Edwards, Information Security Officer, Univ. of Louisville
- Brett Short, Compliance Privacy Officer, Univ. of Kentucky
- John Tarrant, Chief of Medical Staff, Kentucky Dept. of Corrections
- Miriam Paramore, Integra Professional Services
- Martha Sullivan, Information Systems Director, Harrison Memorial Hospital
- Andrew Conkovich, HIPAA Compliance Officer, Kindred Healthcare
- Reese Baker, CIO, Crittenden Health Systems
- Dr. Keith Knapp, CEO, The Episcopal Church Home
- Susan Gitzinger, Director of Professional Affairs, Kentucky Pharmacists Assoc.
- David Bolt, COO, Lewis County Primary Care System
- Tammy Geltmaker, Healthcare Excel
- Kathy Hager, DNP, CFNP, Kentucky Nurses Assoc.
- Kay T. Roberts, Director, Harrambee Nursing Center, Univ. of Louisville
- Jeff Akers, Director of Clinical Pharmacy, Appalachian Regional Healthcare
- Dan Daffron, Pharmacist, Daffron Kwik-Script Pharmacy
- Rosie Maklivic, President, Kentucky Health Department Assoc.

- Sohrab Felfeli and Linda Robinson, CHFS Office of Technology
- Jan Howell, Deputy Commissioner, CHFS Department for Medicaid Services
- Julie McPeak, Deputy General Counsel, Personnel Cabinet
- Dr. Dan Varga, Norton Healthcare

3. Legal Working Group

Chair: Vickie Yates Brown, Member, Greenebaum, Doll, & McDonald
Members:

- Pat Padgett, KMA staff counsel
- Jackie Kingsolver, Greenebaum, Doll, & McDonald
- Marti Arvin, Privacy Officer, Univ. of Louisville
- Paul Herrington, HIPAA Compliance Officer, Humana
- Christy Hendricks, Baptist Healthcare
- Jeff Barnett, Deputy General Counsel and Deputy Executive Director, Certificate of Need, CHFS
- Carolyn Lambert, HIPAA Officer, Brown Forman
- Melissa Metzger, Anthem
- Janet Craig, Stites Harbison
- Margaret Young-Levi, Ephraim McDowell Health

4. Solutions Working Group

Chair: Jeff Rose, Director of Technology Development, Connect Kentucky
Members:

- Ed Forrester, CEO, Management Systems Integration
- Mike Cromika, Director, IS & HIPAA Officer, Western Baptist Hospital
- Karen Stone, Director of Health Information Management, Lourdes Hospital
- Alex Rodriguez, Health Alliance
- Gordon Rohweder, CIO, Owensboro Medical Health System
- Chris Corbin, Executive Director, CHFS Office of Health Policy
- Sohrab Felfeli and Linda Robinson, CHFS Office of Technology
- Toby Whitehouse, Security Administration Branch, COT
- David Montgomery, Systems Design Group Incorporated
- Charlie Kendell, Department for Public Health
- Brenda Beckham, Director Health Information Management, Baptist Hospital East
- Dr. Shawn Glisson, Kentuckiana Cancer Institute
- Vickie Yates Brown, Greenebaum, Doll, & McDonald

Appendix B: Health Information Exchange Scenarios

1. Patient Care Scenario A

The emergent transfer of health information between two healthcare providers when the status of the patient is unsure.
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. 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 inpatient stay.

2. Patient Care Scenario B

The non-emergent transfer of records from a specialty substance treatment provider to a primary care facility for a referral.
A specialty substance abuse treatment facility wants to refer client X to a primary care facility for a suspected medical problem. The client has a long history of using various drugs and alcohol relevant for medical diagnosis. The information is being sent to the primary care provider without the patient's authorization. The primary care provider refers the patient to a specialist and sends all of their information (without patient authorization) including the information received from the substance abuse treatment facility to the specialist.

3. Patient Care Security and Access - Scenario C

At 5:30pm Dr. X, a psychiatrist, arrives at the skilled nursing facility to evaluate his patient, recently discharged from the hospital psych unit to the nursing home. At the time of the patient's transfer, the discharge summary and other pertinent records were electronically transmitted to the nursing home.

Upon entering the facility Dr. X seeks assistance in locating his patient, gaining entrance to the locked psych unit and accessing her electronic health record to review her 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. Unable to access the long-term care 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 the 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 long-term care facility notifies Dr. X's office that they are unable to open the encrypted document because they do not have the encryption key.

4. Patient Care - Scenario D

The non-emergent transfer of health information
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 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 because other family members have had breast cancer.

5. Payment Scenario

X Health Payer (third party, workers compensation, disability insurance, employee assistance programs) provides health insurance coverage to many subscribers in the region the healthcare 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 healthcare provider's workforce members and medical staff members and their office staff.
X Health Payer is requesting access to the EHR by its case management staff to approve/authorize inpatient encounters.

6. RHIO Scenario

The RHIO in your region wants to access 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.

7. Research Data Use Scenario

A research project on children younger than age 13 is being conducted in a double blind study for a new drug for ADD/ADHD. The research project is being reviewed by the IRB that presides over research protocols at the major medical center where the research investigators are located. The data being collected are all electronic and all responses from the subjects are completed electronically in the same data base file.

The principle investigator was asked by one of the investigators if they could use the raw data to track the patients over an additional six months or use the raw data collected for a white paper that is not part of the research protocols final document for his post doctoral fellow program.

8. Scenario for access by 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 arrives in the ER in addition to the patient's parents. 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 are made to the ER staff. The patient is covered under their parent's health and auto insurance policy.

9. Scenario A Pharmacy Benefit

The Pharmacy Benefit Manager (PBM) has a mail order pharmacy and also has a closed formulary. The PBM receives a prescription from Patient X 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.

10. Scenario B for Pharmacy Benefit

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 their prescription drug benefit. Company A is self-insured and as part of their current benefits package, they have the prescription drug claims submitted through their current PBM (PBM2). PBM1 has requested that Company A send their electronic claims to them to complete the review.

11. Healthcare Operations and Marketing - Scenario A

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.

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:

1. To provide information on the hospital's new pediatric wing/services.
2. To solicit registration for the hospital's parenting classes.
3. To request donations for construction of the proposed neonatal intensive care unit
4. They will sell the data to a local diaper company.

13. Bioterrorism event

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 public to symptoms and seek treatment if feel affected. The State also notifies the Feds 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.

14. Employment Information Scenario

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 2 days leave. The hospital ED has an EHR and their practice is to cut and paste patient information directly from the EHR and transmit the information electronically to the HR department.

15. Public Health - Scenario A--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.

16. Public Health - Scenario B--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.

17. Public Health Scenario C--Homeless shelters

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.

18. Health Oversight: Legal compliance/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 healthcare 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.