

HISPC

Health Information Security and Privacy Committee State of Nebraska

Security and Privacy Barriers to Health Information Interoperability

Final Report for the state of Nebraska
June 2007



Partial resources support from the Creighton Health Services Research Program (CHRP) and grant no. 1P20 HS015816 Building Research Infrastructure Capacity from the Agency for Healthcare Research and Quality (AHRQ); and the State Offices of Rural Health grant no. H95RH00119, Nebraska Health and Human Services System

Security and Privacy Barriers to Health Information Interoperability

Table of Contents

Executive Summary	3
HISPC Committee Members	
Steering Committee Members	7
HISPC-RFP State of Nebraska Internal Project Team	7
HISPC Steering Committee Consultants	7
Background	
Issue	8
Federal and State Statutes, Business Practices and Patient Consent	9
Summary of Key Findings of HISPC Report 1: Survey of Health/ Licensure/Certification and Facilities Oversight Board Managers.....	11
Summary of Key Findings Report 2: Survey of Health Professions Organizations Leadership	11
Summary of Key Findings Report 3: Consumer Views about Privacy and Electronic Health Information Exchange	12
State Progress and the Larger National Context.....	13
Federal and Nebraska Initiatives to Move Health Information Technology Forward.....	13
Progress in the Adoption of Health Information Technology and Data Exchange	15
Consumer Perspectives	17
Security and Privacy Issues	17
Findings and Recommendations	19
References.....	22
Appendices	
A. Charter: State of Nebraska eHealth Council.....	24
B. Nebraska Initiatives in Health Information Technology and Patient Safety.....	29
C. Resources	33
D. Taxonomy for Health Care and Information Technology Professionals.....	37
E. Taxonomy for Consumers	52

HISPC

Health Information Security and Privacy Committee State of Nebraska

Security and Privacy Barriers to Health Information Interoperability

Executive Summary Final Report for the state of Nebraska

The United States is in the middle of a ten year plan to develop and implement a nationwide electronic health information infrastructure that will allow authorized health care professionals to securely access relevant patient data from any location in the country at any time. As envisioned, the National Health Information Initiative in the United States will be a “series of cross-jurisdictional interconnected regional health information exchanges or organizations”.¹ The Lieutenant Governor for the State of Nebraska formed the Health Information Security and Privacy Committee (HISPC) in 2006. The vision driving the state HISPC is to create the flexibility to electronically exchange patient authorized health care information, confidentially and securely between the patient/client and all appropriate persons involved in the health care process. Many issues have come to light nationwide as states begin to work on these linkages and collaborations. One core issue is how to appropriately protect the privacy and security of health information in an interconnected electronic health information system. The Nebraska HISPC has focused its energy on the issue of “privacy”, believing that security is an issue that lies outside of a single state’s ability.

The HISPC has reviewed key documents related to the state statutes that address, movement of personalized health information to assist in the treatment and care of a patient. We have also conducted surveys of three stakeholder groups in Nebraska: 1) health/licensure/certification and facilities oversight board managers, 2) health professions organizations leadership, and 3) consumers. These surveys assessed stakeholder security and privacy issues as they relate to stakeholder knowledge and perception about health information exchange, technology, and quality and safety of patient care. These state level findings are then presented in comparison to the nation when feasible, as determined through a review of national reports, publications and technical information from leading health information organizations and the government.

This final report reflects a benchmark about the progress toward health information exchange and overcoming security and privacy barriers in the state of Nebraska as compared to the nation. The HISPC committee has identified a fundamental need for a *sustainable* process of monitoring and facilitating the assurances of privacy and security as both the entities in the state and the state government continues to increase in capacity for health information exchange. Researchers must continue to play a key role in assisting us to gain new knowledge as we move forward. Our findings in the state were consistent with in the 33 state examination of security and privacy issues released in June of 2007, whose findings are summarized in our full report.²



Partial resources support from the Creighton Health Services Research Program (CHRP) and grant no. 1P20 HS015816 Building Research Infrastructure Capacity from the Agency for Healthcare Research and Quality (AHRQ); and the State Offices of Rural Health grant no. H95RH00119, Nebraska Health and Human Services System

¹ Substance Abuse and Mental Health Services Administration (SAMSHA): the Implementation of E-consent Mechanisms, Feb. 16, 2007

² Dimitropoulos, L.L. Interim assessment of variation: privacy and security solutions for interoperable health information exchange. December 29, 2006. RTI Project No. 0209825.000.004.002 RTI International, Chicago, Illinois.

Recommendations are provided. The magnitude, complexity, and dynamic nature of the developing health information exchange efforts in the state have guided these recommendations. These factors also influenced the committee to develop this report as an educational resource document that offers guidance to health and information technology (IT) professionals while also assisting consumers of health care with some basic understanding of terms and concepts about security, privacy and health information exchange.

The final findings and recommendations of the HISPC Committee are:

Finding 1: Facilitation of knowledge and understanding about health information exchange is essential for the Nebraska Health and Human Services Health Board managers and Facility Oversight Managers. This knowledge directly affects the management of security and privacy issues. Managers who are equipped with this understanding can assist the boards to address how current and future rules and regulations affect and are affected by the evolving landscape of health information exchange and interoperability.

Recommendation:

- **Nebraska Health and Human services develop a process for obtaining timely and up to date technical information on health information and interoperability and disseminating this to health/ licensure/ certification board managers and their members.**
- **Nebraska Health and Human services charge managers to facilitate the boards to address how current and future rules and regulations affect and are affected by the advancement of health information exchange and interoperability.**

Finding 2: Facilitation of knowledge and understanding of health professionals across the state is an important role that the health professions organizations can perform. These organizations vary in their engagement and understanding of the technical information about health information interoperability and the related security and privacy issues. The organizations would provide a great service in the process of informing their members about understanding health information exchange and interoperability, and the related security and privacy practices and issues.

Further, the unique knowledge and expertise of health care practitioners, facilities in which health care is provided, organizations involved with health issues at the societal level and educators of health professions students, is needed to address how current laws, rules and regulations related to their disciplines affect and are affected by the electronic exchange of health information. We encourage these associations to seek additional information about health information exchange and interoperability in other regions within the state, region, nationally and internationally.

Recommendation:

- **the e-Health Council engage all health professional associations involved in health care delivery and services to assist in present and future efforts to design, implement and educate key stakeholders in the health professions, health education and health organizations about the sharing of health information, and the related security and privacy issues as these processes unfold.**

Finding 3: The HISPC recognizes that state government, boards and health care providers need more knowledge about the Nebraska consumer. Consumer viewpoints are critical to this broader understanding of health information exchange and interoperability. A larger and broader representation of consumer viewpoints and needs will greatly improve our understanding of “what” consumers will participate in and “how” they will participate.

Similarly, consumers are in great need of information and education about health information exchange and interoperability. Consumers have concerns that must be addressed through knowledge dissemination. This will facilitate the best decision-making possible for the consumer. A dissemination process for essential and timely information related to progress of this initiative occurring at both the federal and state level to consumers is needed.

A variety of ways of consumer involvement are needed to assist in the design of the processes of education of all stakeholders and policy formulation as the macro system of sharing health information electronically unfolds over time. This is an essential step to facilitating citizens and providers to more easily establish a common understanding and agreed upon set of solutions to health information exchange as security and privacy issues are addressed.

Recommendation:

- **The e-Health Council engage consumers to assist in present and future efforts to design, implement and educate other consumers and key stakeholders in the health professions, health education and health organization about the sharing of health information, and the related security and privacy issues as these processes unfold.**

Finding 4: The complexity of the rules and regulations create confusion in the area of privacy. Because the HIPAA preemption rules are complex, individuals in a position to potentially disclose protected health information (PHI) sometimes are unsure if the PHI may be disclosed without written individual authorization. Health care providers and payers who are faced with potential civil and criminal HIPAA fines and penalties, state law causes of action for invasion of privacy, and reporting to licensure boards for breach of confidentiality, may often decide not to disclose PHI without written patient authorization, when it is otherwise permissible to disclose.

Recommendation:

- **The e-Health Council should study the issues identified and described in the background information of this report and recommend a sustainable action plan developed to facilitate progress in assuring privacy and security protections of the individual while progressing in health information exchange.**

Finding 5: Our HISPC study of security and privacy issues is consistent with the same concerns and areas of work needing to be addressed within our state and its’ communities as a most recent cross-sectional study of the nation revealed.¹ The issues are embedded in complexity and confusion associated with state and federal level inconsistencies, conflicting business practices, and varying

¹Dimitropoulos, L.L. Interim assessment of variation: privacy and security solutions for interoperable health information exchange. December 29, 2006. RTI Project No. 0209825.000.004.002. RTI International, Chicago, Illinois. (ref. 16)

consent policies and approaches. These issues must be untangled and addressed. This will require a sustained commitment to achieve.

Recommendation:

- **The e-Health Council should explore the development of a sustainable system for monitoring our progress in studying and addressing the security and privacy issues within the state of Nebraska.**
- **An in-depth study of existing laws and regulations, with guidance from representatives from health professions, health educators and health organizations is needed to develop solutions on how to overcome these barriers.**

Finding 6: Based on the three research reports from this committee and our discussions, we believe there is a need for further research needed about implications to consumers, health professionals, health systems, educators, private and public care providers, and payers. Examples of important research questions that the committee has thought about, but are not limited to include:

- How are consumer's health and safety outcomes affected by the sharing of health information?
- What processes are necessary for consumers to participate in the sharing of health information?
- How will consumers concerns about the risks they perceive with health information sharing be "stewarded" as the processes emerge, and who will "steward" them?
- How are small business health care providers, health systems and large healthcare organizations, affected by the impact of sharing health information: What is the impact on workload? What is the impact on workforce considerations?
- How will the educational needs of the young, middle age, young-old and old-old adults be met as these processes develop?
- What is the impact of a partial adoption of health information sharing on patient security and privacy?

Recommendation:

- **The NHHS should pursue further research in the area of how to obtain needed technical information and employ effective processes of applying this information to assist health boards and facility boards with the ongoing process of staying current in and facilitating adoption of future rules and regulations that advance secure, private health information and interoperability approaches.**
- **Further research should be conducted by professional organizations about the on-going impact of health information and exchange and interoperability on provider and patient security and privacy issues.**
- **Further research should be conducted to better understand consumer viewpoints and needs.**

HISPC Steering Committee:

- ◆ Lieutenant Governor Rick Sheehy
- ◆ Senator Pat Bourne (Past Member)
- ◆ Senator Jim Jensen (Past Member)
- ◆ Senator Philip Erdman
- ◆ Mark Adams, Corporate Security Officer, Blue Cross/Blue Shield of Nebraska
- ◆ Brenda Decker, Chief Information Officer, State of Nebraska
- ◆ David H. Filipi, M.D., Vice President, Medical Affairs, Physicians Clinic
- ◆ Kimberly Galt, Pharm.D., F.A.S.H.P., Associate Dean of Research, School of Pharmacy and Health Professions and Director, Creighton Health Services Research Program (CHRP)- Creighton University
- ◆ Steve Grandfield, Exec. Vice President, Blue Cross/Blue Shield of Nebraska (Past Member)
- ◆ Donna K. Hammack, Chief Development Officer, St. Elizabeth Foundation
- ◆ Steven H. Hinrichs, M.D., Professor/Director, UNMC – Dept. of Pathology/Microbiology
- ◆ Ron Hoffman, RHU, S5-Enterprise Privacy Office, Mutual of Omaha Insurance Company
- ◆ Dick Nelson, Director, NE HHSS – Dept. of Finance & Support (Past Member)
- ◆ Nancy Shank, Associate Director, University of Nebraska Public Policy Center
- ◆ September Stone, R.N., Nebraska Health Care Association
- ◆ Joni R. Cover, J.D., Executive Vice President, Nebraska Pharmacists Association
- ◆ Rick Zarek, R.P. (Past Member)

HISPC-RFP State of Nebraska Internal Project Team:

- ◆ Dennis Berens, Director, Nebraska Office of Rural Health NE HHSS – Dept of Regulation & Licensure (Facilitator)
- ◆ Joseph Acierno, M.D., J.D., Deputy Chief Medical Officer, NE HHSS – Dept of Regulation & Licensure
- ◆ Jacqueline Miller, DDS, Deputy Director, NE HHSS – Dept of Regulation & Licensure
- ◆ Roger Brink, J.D., Legal Counsel, NE HHSS – Dept of Finance & Support
- ◆ Harry Farley, Legal Services, NE HHSS – Dept of Finance & Support
- ◆ David Lawton, R.N. Ph.D., Health Surveillance Administrator, Public Health Assurance/Bioterrorism, NE HHSS – Dept of Regulation & Licensure
- ◆ Bob Leopold, Public Health Assurance/Bioterrorism, NE HHSS – Dept of Regulation & Licensure
- ◆ Dan Noble, M.D., Deputy Chief Medical Director, NE HHSS – Dept of Regulation & Licensure (Past Member)
- ◆ Jim Ohmberger, Administrator Information Systems & Technology Division, NE HHSS – Dept of Finance & Support
- ◆ Kathie Osterman, Administrator Communications & Legislative Services Division NE HHSS – Dept of Finance & Support
- ◆ Jane McGinnis, Managed Care Epidemiologist, Public Health Assurance/Bioterrorism, NE HHSS – Dept of Regulation & Licensure

Consultants:

- ◆ Sheila A. Wrobel, Chief Compliance Officer UNMC – Dept. of Pathology/Microbiology
- ◆ Pat Pankoke, Administrative Assistant, Public Health Assurance/Bioterrorism, NE HHSS – Dept of Regulation & Licensure (Past Member)
- ◆ Kevin Cueto, IT Consultant, Green Iris Technologies, Inc.
- ◆ John A. Glock, IT Project Coordinator, UNMC Public Health Laboratory
- ◆ Karen A. Paschal, P.T., D.P.T., Associate Professor of Physical Therapy, Creighton University
- ◆ Whitney Shipley, Program Coordinator UNMC – Center for Biopreparedness Education (Past Member)

Report Prepared by:

- ◆ Dennis Berens, Kimberly Galt, Pharm.D, F.A.S.H.P., and Karen A. Paschal, P.T., D.P.T. The assistance of Ms. Jamie Barbee of the Creighton University Health Services Research program with data collection and report preparation is acknowledged.

Security and Privacy Barriers to Health Information Interoperability Final Report

Background

Issue

The United States is in the middle of a ten year plan to develop and implement a nationwide electronic health information infrastructure that will allow authorized health care professionals to securely access relevant patient data from any location in the country at any time. As envisioned, the National Health Information Infrastructure (NHII) in the United States will be a “series of cross-jurisdictional interconnected regional health information exchanges or organizations”.¹ The Lieutenant Governor for the State of Nebraska formed the Health Information Security and Privacy Committee (HISPC) in 2006. The vision driving the HISPC is to create the flexibility to electronically exchange patient authorized health care information, confidentially and securely between the patient/client and all appropriate persons and entities involved in the health care process.

Many issues have come to light nationwide as states begin to work on these linkages and collaborations. One of the core issues is how to appropriately protect the privacy and security of health information in an interconnected electronic health information system. This involves a renewed focus on the HIPAA standards and the statutes, rules and regulations found in each state. Sensitive health information and a variety of laws requiring specific patient consent to disclose information are the focus of many states as they search for connectivity of health information.

The HISPC has reviewed key documents related to state statutes that address, movement of personalized health information to assist in the treatment and care of a patient. We have also conducted surveys of three stakeholder groups in Nebraska: 1) health/licensure/certification and facilities oversight board managers, 2) health professions organizational leadership, and 3) consumers. These surveys assessed stakeholder security and privacy issues as they relate to stakeholder knowledge and perception about health information exchange, technology, and quality and safety of patient care. The three reports are available that describe the detailed results of each of these areas, and key findings from each report. The overarching recommendations are summarized in this final report.^{1, 2, 3} These state level findings are then presented in comparison to the nation when feasible, as determined through a review of national reports, publications and technical information from leading health information organizations and the government.

This final report reflects a benchmark about the progress toward health information exchange and overcoming security and privacy barriers in the state of Nebraska as compared to the nation. The HISPC committee has identified a fundamental need for a *sustainable* process of monitoring and facilitating the assurances of privacy and security as both the entities in the state and the state government continues to increase in capacity for health information exchange. Researchers must continue to play a key role in assisting us to gain new knowledge as we move forward. Our findings in the state were consistent with in the 33 state examination of security and privacy issues released in June of 2007, whose findings are summarized in our full report.²

¹ Substance Abuse and Mental Health Services Administration (SAMSHA): the Implementation of E-consent Mechanisms, Feb. 16, 2007

²Dimitropoulos, L.L. Interim assessment of variation: privacy and security solutions for interoperable health information exchange. December 29, 2006. RTI Project No. 0209825.000.004.002 RTI International, Chicago, Illinois.

Recommendations are provided. The magnitude, complexity, and dynamic nature of the developing health information exchange efforts in the state have guided these recommendations. These factors also influenced the committee to develop this report as an educational resource document that offers guidance to health and information technology (IT) professionals while also assisting consumers of health care with some basic understanding of terms and concepts about security, privacy and health information exchange.

Federal and State Statutes, Business Practices and Patient Consent

The federal and state laws, business practices, and patient consent issues are major areas that emerged in the HISPC committee exploration and evaluation of security and privacy issues in the state.

Both federal and state laws govern health information exchange. Primary federal laws include the Health Insurance Portability and Accountability Act of 1996 (HIPAA) at 45 CFR 160-164 and the Confidentiality of Alcohol and Drug Abuse Patient Records regulations at 42 CFR Chapter 1 Part 2. Nebraska has several laws that permit disclosure of health information without written patient authorization. Most of these laws are in the area of public health, and include but are not limited to infectious disease reporting to the public health department, disease/health condition registries, workers compensation, and child/dependent adult abuse reporting. There are also relevant aspects of the law in both the Professional and Occupational Licensure and the Health Care Facilities and Services Licensure Nebraska Administrative Code. Finally, each of the health –related professions has a body of law that addresses privacy and security.

The impact of HIPAA is one of the primary laws that must be addressed in this effort. The federal HIPAA preempts state privacy laws that are less stringent. “Less stringent” means that the state law either affords the individual with less privacy protection, or fewer privacy rights. Preemption is a doctrine adopted by the U.S. Supreme Court holding that certain matters are of such a national, as opposed to local character that federal laws pre-empt or take precedence over state laws. A state may not pass a law inconsistent with the federal law. HIPAA-covered entities must either follow HIPAA or a more stringent state law. In order to comply with HIPAA, covered entities must analyze each state privacy law, and determine whether it is more or less stringent than HIPAA. Most states, including Nebraska, have model preemption analysis so that all covered entities generally interpret laws the same way.

The Nebraska Hospital Association published an analysis of the HIPAA preemption in 2003. The primary source document was contracted for preparation by the Nebraska Hospital Association. The document is entitled, “NHA: Updated HIPAA Preemption Analysis for Providers.”⁴ The purpose of the document is a planning/reference document to help covered entities understand which law applies when the mandates of HIPAA interact with State Law. The 103 page document covers 16 categories of health-related state laws that address, the movement of personalized health information to assist in the treatment and care of a patient. The HISPC committee has reviewed this key document and observed that there are detailed inconsistencies in the state law that will need to be addressed in order to move forward with health information exchange. Examples of issues identified as possible barriers to health information exchange include: 1) some licensure regulations for facilities set a higher standard and do not allow permissive disclosures, 2) some state laws have not envisioned electronic records and only address the paper form of records, and, 3) there are timeliness issues about patients’ rights to medical record release that may be problematic. A

systematic evaluation of the findings of this report with a resultant action plan for the essential areas that must be addressed is needed.

Because the HIPAA preemption rules are complex, individuals in a position to disclose protected health information (PHI) sometimes are unsure if the PHI may be disclosed without written individual authorization. Health care providers and payers, faced with potential civil and criminal HIPAA fines and penalties, state law causes of action for invasion of privacy, and reporting to licensure boards for breach of confidentiality, may often decide not to disclose PHI without written patient authorization, when it is otherwise permissible to disclose. For example, under HIPAA, covered entities may disclose PHI to another health care provider without individual authorization if both have a treatment relationship with the individual.

We do not yet know what the risks are to individuals and organizations based upon case law. HIPAA regulations prohibit individuals from initiating a law suit when a breach of security or privacy has occurred. Subsequently, the risks to individuals, consumers, health professionals and organizations are uncertain. This risk will unfold as we move through greater implementation of health information exchange practices.

In October 2005, federal Stark and Anti-Kickback Amendments that support adoption of e-prescribing and electronic health records were proposed. The Centers for Medicare and Medicaid Services proposed to create exceptions to the “physician self-referral” law to allow hospitals and certain health care organizations to furnish hardware, software, and related training services to physicians for e-prescribing and electronic health records, particularly when the support involves systems that are “interoperable” and thus can exchange information effectively and securely among health care providers. In a parallel action, the Office of the Inspector General (OIG) announced proposed safe harbors for arrangements involving the donation of technology for e-prescribing and electronic health records. Arrangements for the provision of items and services that meet the requirements of the safe harbors would be exempt from enforcement.

The concept of “safe harbor” should be further explored to assist individuals and corporations with resolving risk related to disclosure and other actions related to PHI exchange. The concept of unprofessional conduct should also be explored and addressed in this context. State laws, and their interpretation in the rules and regulations governing each health care provider or organization, must be modified or addressed explicitly within these areas of complexity. The inconsistencies between federal HIPAA laws and state laws may lead to the interpretation of health information exchange being deemed in violation, possibly under the circumstances where a patient has given permission to share personal health information. What is common practice in health care organizations and professional practices may be in violation. These points must be addressed and will require the involvement of the relevant professions or health organizations.

Appropriate “opt-out and opt-in” and “consent mechanisms” are needed to assure the privacy and security of the citizens’ health information as increasing health information exchange practices occur. All of the points where patients can control their information should be explicitly identified and the appropriate consent mechanisms aligned. Opt-in may be appropriate today but opt-out may be the choice later when patients are more aware of the issues. The banking industry is a good example of this transition. People transitioned from an unwillingness to use electronic information to conduct banking to routine paperless transactions. Will our citizens view the health care industry similar to the banking industry with respect to information management?

Summary of Key Findings of HISPC Report 1: Survey of Health/Licensure/Certification and Facilities Oversight Board Managers

Almost all Nebraska HHS managers represent groups that have health information that would be part of a patient/client/consumer comprehensive health record or information of importance to public health reporting and tracking. Conversation takes place about health information privacy in the context of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), but not electronic health record exchange. Knowledge about data exchange entities, such as regional health information organizations (RHIO), is lacking in this area of our public health. Most board managers report that the rules and regulations prohibit releasing confidential information about a patient without the patient's permission. However the board manager representing Audiologists and Speech-Language Pathology described an interesting requirement: transfer of care must occur to another health care professional and it is unprofessional conduct to not facilitate this when needed. It is worth further exploration about how this is achieved while still maintaining confidentiality.¹

Summary of Key Findings Report 2: Survey of Health Professions Organizations Leadership

Most health profession association leaders are aware of the federal initiative to achieve health information interoperability. However, they are generally not familiar with data exchange entities such as Regional Health Information Organizations (RHIOs). Most professions have practice acts that address both: 1) a professional's responsibility toward privacy and confidentiality of patient information, and 2) a professional's responsibility for sharing release of patient/client health information records to individuals other than the patient/client. From the professional practitioner's eyes, patients keep track of health information on paper. However, early signs of health information technology (HIT) use by patients are present. Security and privacy barriers were most frequently described in relationship to the Health Insurance Portability and Accountability Act (HIPAA) rather than initiatives related to electronic health records. Solutions to these barriers offered by respondents include changing legislation or providing education.

Barriers to health information exchange exist conceptually from both a personal and professional viewpoint. These barriers are generally recognized as increased risk through 1) unnecessary access to information others do not need, 2) violations of privacy, 3) increased medical errors due to interpretation problems (information used the wrong way), and 4) getting patients' records confused. There is an element of mistrust that the technology and systems will be dependable. Concerns about assuring privacy of health information centered on data security, on what content specifically is at risk, and on having up-to-date information when it is accessed.

The sharing of health information is embraced with some caution. Professionals will share the information they obtained from other practitioners with their patients, citing respect for the patient as the primary owner of the information. The great majority of respondents are willing to share their patient's electronic health information with other providers if the patient gave permission. Most indicated they would be willing to share a wide range of data. Overall, health professional association leadership supports information exchange believing that patient care quality and safety will improve. Overwhelmingly, the professions believe that having an electronic health record in their own practice environment will improve both the overall safety and quality of healthcare. They just as strongly believe that sharing Electronic Health Records (EHRs) will do the same.

The individuals who are experts about health information exchange (HIE) in Nebraska do not appear to overlap with the leadership of organizations representing health care professionals. There has not yet been integration of an action-orientation to advancing the HIE initiative within these organizations.²

Summary of Key Findings Report 3: Consumer Views about Privacy and Electronic Health Information Exchange

The need for consumer education, engagement and empowerment in the process of implementing a health information exchange that meets the security and privacy rights and needs of consumers is recognized by the federal government. The Secretary of HHS has been meeting with major employers throughout the country to engage them in an effort to empower consumers through information. These efforts were further supported by the President's Executive Order 13410, issued on August 22, 2006, requiring that all federal agencies and those who do healthcare business with the government do the following: 1) Aggregate healthcare quality and price information so that it is available to beneficiaries, enrollees and providers in a readily usable manner; 2) Use interoperable HIT products in order to aggregate and share quality and price data; and 3) Motivate participants to become consumers and advocates of a HIT healthcare system.⁵

Our survey research in Nebraska indicates that there is a great need for consumer education and engagement here. The combination of data received through surveys and interviews expresses a here-to-fore missing voice in the discussion of security and privacy barriers to health information interoperability. The voices of consumers are critical as we move to the electronic management and exchange of health information. Consumers have unique perspectives on security and privacy. There is plurality in their identified concerns and needs. To achieve full engagement, multiple approaches to addressing their perceived needs will be necessary. Consumers fear medical identity theft, which is substantiated by the 200,000 cases of medical identity theft in 2003.⁶ However, overall, consumers are focused on the belief that personal health care information should be shared to improve their care. As promoters, developers and planners, we must be able to answer their questions and concerns.

Preliminary data indicates a lack of consumer knowledge and misperceptions about the current management of health care information as well as future electronic management and exchange. This is consistent with other trade industry studies. Most consumers are unaware of all the ways health information is used once access has been granted to a provider or third party payer. Without complete and accurate information, consumers may make decisions that are not in their best interest.

We know a little about consumer viewpoints now, but we need to know more. The six individuals interviewed represent the major ethnic, age, socioeconomic and severity of illness characteristics that are typically considered "diverse". However, we learned through this work that "relevant diversity" is broader. Care continuum, care settings, and other access issues are highly important to learn about in order to understand the consumers' viewpoints and needs. We need to know more than we know about consumers in our state.

Consumer knowledge is represented at a higher level by this group of consumers than is likely in the state. The sample of consumers who participated is more informed as a result of their advisory role to the quality improvement organization in the state. We are likely to have received the "best picture", not the "average picture".³

Education and leadership are both needed to help health care providers and consumers understand the need for quality information to be exchanged, i.e. move from discontinuous care to continuity of care approaches. This is necessary in order to attain improvement in health care service quality. A formal education model is needed that links these concepts for all stakeholders. A variety of approaches are needed depending on the type of record, i.e., electronic health record vs. personal health record that is adopted.

State Progress and the Larger National Context

A scan of the national work being done in the areas of health information exchange and technology was conducted in late 2006 and early 2007. Key observations of the published literature and reports help us understand the state of Nebraska in relationship to the nation.

Federal and Nebraska Initiatives to Move Health Information Technology Forward

In 1999, the Institute of Medicine (IOM) report, *To Err is Human*, was released.⁷ The landmark report provided substantial evidence for the need to reduce harm in our medical care systems by implementing safety concepts and practices, including the use of medical technologies. In 2001, the Secretary for Health and Human Services appointed The Patient Safety Task Force as a part of the Secretary's Quality Improvement Initiative for the nation. Representation was formed from four federal agencies: Agency for Healthcare Research and Quality (AHRQ), Centers for Disease Control and Prevention (CDC), Food and Drug Administration (FDA), and the Centers for Medicare & Medicaid Services (CMS). This task force was charge to coordinate, communicate and conduct research, demonstration projects, and quality improvement programs aimed at promoting patient safety, as well as, monitor rates of risk factors and actual patient harm. Consumers concerns continued while this federal effort was initiated. A 2004 Kaiser Family Foundation survey of consumers found 40 percent were very concerned about serious errors or mistakes when they received care from the doctor's office.⁸

By 2005, the HHS Secretary Leavitt announced the formation of the American Health Information Community (the Community), a national public-private collaboration formed pursuant to the Federal Advisory Committee Act. The Community was formed to facilitate the transition to interoperable electronic health systems in a smooth, market-led way. The Community provides input and recommendations to the Secretary on use of common standards and how interoperability among Health IT systems can be achieved while assuring that the privacy and security of those records are protected. The Community was chartered for two years, with the option to renew for a total of no more than five years. The DHHS intends for the Community to be succeeded within the five years by a private-sector health information community initiative that, among other things, would set additional needed standards, certify new health information technology, and provide long-term governance for health care transformation.

In 2006, the federal government administered a contract through the Agency for Healthcare Research and Quality (AHRQ) to conduct a cross-sectional study of issues of security and privacy in the states and territories. This project is entitled the Health Information Security and Privacy Collaboration, (HISPC) discussed in greater detail in the next section.

In 2006, the National Governors Association was also contracted by the Office of the National Coordinator for Health Information Technology (ONCHIT) to provide advisory services for health

information exchanges as they developed in the various states.¹⁰ From this emerged the State Alliance for e-Health with the following charges:

- From a state-specific perspective, address barriers to health information exchange and adoption of health IT, while preserving privacy, security, and consumer protections.
- Build consensus in seeking the harmonization of the variations in state policies, regulations, and laws, where appropriate, and develop standards and/or guidance for modifying such policies, regulations, or laws.
- Allow for dialog among states that will fuel creativity and partnerships among states and with the private sector in the health IT arena.
- Allow for the appropriate input of experts and others working on health IT endeavors to inform state policymaking.

Three task forces function under the alliance: 1) the Health Information Protection Taskforce, 2) the Health Care Practice Taskforce, and 3) the Health Information Communication and Data Exchange Taskforce. These task forces address: 1) privacy and security issues through input from the Privacy and Security Contract and any follow-up work in states, 2) work through state licensure laws that hinder ability to engage in health information exchange and telemedicine; medical malpractice, including medical record and liability issues, and 3) analyze appropriate states roles in models for HIE; explore means to integrate state-level HIE with public health programs; identify public funding opportunities and priorities, respectively. Other task forces deemed useful may be added, or issues that emerge will be integrated into the existing groups.

The HHS also awarded a contract to the American National Standards Institute (ANSI), a non-profit organization that administers and coordinates the U.S. voluntary standardization activities, to convene the Health IT Standards Panel (HITSP). The goal of HITSP is to develop and implement a useful set of health IT standards that will support interoperability among healthcare software applications, including EHRs, and be widely accepted. HITSP is finalizing recommendations on HIT standards for three key “use cases” – (1) submission of laboratory test results to an EHR; (2) submission of bio-surveillance data from providers and hospitals to public health agencies; and (3) automated patient registration information and medical history used in personal health records (PHRs).⁹

In a similar time frame, several Nebraska state level initiatives and actions have taken place. A timetable of events and structures that formed in response is shown here:

2003	<p>Nebraska Coalition for Patient Safety</p> <ul style="list-style-type: none"> ▪ A statewide partnership established to ensure the safety of all individuals who seek healthcare in Nebraska’s healthcare facilities or from Nebraska’s healthcare professionals.
2005	<p>LB361 Patient Safety Improvement Act</p> <ul style="list-style-type: none"> ▪ Formation of broad based patient safety organization
2006	<p>Nebraska Health Information Security and Privacy Committee (HISPC)</p> <ul style="list-style-type: none"> ▪ Lieutenant Governor appointed committee to evaluate and examine the security and privacy issues and responsibility to citizens with HIT <p>Nebraska Telehealth Network</p> <ul style="list-style-type: none"> ▪ The Nebraska statewide telehealth network connects nearly all of the state's hospitals and public health departments.

2007	<p>State of Nebraska e-Health Council</p> <ul style="list-style-type: none"> ▪ The eHealth Council was created by the Nebraska Information Technology Commission (NITC) as a subcommittee, under the leadership of the Lieutenant Governor in early 2007 (www.nitc.state.ne.us/eHc/about.html). The purpose of the Council is to facilitate discussions among eHealth initiatives in the state and to make recommendations to the NITC regarding the adoption and interoperability of eHealth technologies.
------	---

Progress in the Adoption of Health Information Technology and Data Exchange

Several academic researchers/institutions and organizations have obtained competitively funded research and project planning and implementation grants that have supported the early formation of RHIOs, large scale quality improvement and safety programs, and exploration and study of adoption of health information technology use by health care providers and patients. An overview of these projects is shown in Appendix A, Nebraska Initiatives in Health Information Technology and Patient Safety.

Formation of state RHIOS and other data exchange organizations. Three projects have been funded by the federal government based upon program planning and implementation grants. The first project, *Western Nebraska Health Information Exchange* is well on its way to implementing a regional health information exchange (RHIO). A planning grant from the U.S. Department of Health and Human Services Agency for Healthcare Research and Quality (AHRQ) in 2004 enabled partners to begin the planning process. In 2005, a three-year implementation grant from AHRQ was awarded. A HRSA Rural Network Development Grant has provided the opportunity to expand this regional work to Panhandle Community Services Health Center, private physician’s clinics, long term care, and others. The University of Nebraska Public Policy Center is the Principle Investigator for the AHRQ grant, providing research and consultation on the project design. Partners have met with state agencies to discuss how the regional health information exchange being developed can interface.

The second project is the *Southeast Nebraska Behavioral Health Information Network*, a \$200,000 one-year planning grant from the U.S. Department of Health and Human Services Agency for Healthcare Research and Quality (AHRQ) awarded in 2004. This enabled Region V Behavioral Health Care Providers to develop a plan for a health information technology infrastructure that will result in standards-based data sharing and lead to measurable and sustainable improvements in patient safety and quality of care in the region. Fifteen organizations providing behavioral health care in Southeast Nebraska have been identified as potential participants in the Southeast Nebraska Behavioral Health Information Network (SNBHIN—pronounced SIN bin). Since the completion of the planning grant, SNBHIN partners have continued to meet and are making progress toward establishing a RHIO. An RFP has been issued and the group is looking at submitting proposals for additional funding.

The third project is the *Nebraska Health Information Initiative (NeHII)*, a collaboration of Nebraska health care organizations, hospitals, physicians, Blue Cross and Blue Shield of Nebraska, and universities. The mission of the NeHII Collaborative is to provide Nebraska a system for the secure exchange and use of health information.

State Telehealth Network Progress. The Nebraska Statewide Telehealth Network is an interactive video and data network that provides integration among nearly all of the state's hospitals and public

health departments. The Nebraska Statewide Telehealth Network is unrivaled in scope by any other state telehealth network. The Telehealth Governing Board is providing leadership for the network. A total of 8,388 participants used videoconferencing from a hospital or public health department site, saving over \$1,662,000 in travel time and over \$1,645,000 in mileage costs. Over 800 educational programs were presented; over 550 meetings were held; and 687 patient consults were performed using the Nebraska Statewide Telehealth Network in 2006.

Adoption of Electronic Health Records. National research has estimated that between 17 and 25% of physician practices are currently utilizing EHRs and that EHR implementation differs considerably when taking into account size of practice.¹⁰ A study of the state of Nebraska being conducted by the Nebraska Medical Association with the support of the Creighton Health Services Program is in progress to describe the state of electronic medical record (EMR) adoption in physician office-based practices within the state of Nebraska. A cross-sectional survey was distributed to all licensed physicians in the state of Nebraska in February through May of 2007 to identify the stage of EHR adoption of active ambulatory physician office-based practices. There were 1274 respondents for a final response rate is 47.8%. Of these, 11% of physicians have no plans to adopt EHR, 32% are still evaluating the need for EHR in their practice, 16% are currently selecting an EHR system to implement, 17% are in the process of implementing EHR, and 23% of physicians have fully implemented EHRs in their practice. This distribution is compared to national findings conducted two years prior in 2005 indicating that 42% of physician offices did not plan to implement EHRs within the next two years, 35% did plan to adopt it in the next 2 years, 13% are in the process of implementing EHRs, and 12% have fully implemented EHRs. The proportion of physician practices that have implemented EHRs is comparable to the national rate. The Nebraska Medical Association is facilitating the process of working with physician practices across the state for preparation of integrating EHRs through the project, “Enhancing Clinical Practices through the Adoption of Health Information Technology in Nebraska” through a town hall educational process. The NMA is working collaboratively with the Creighton Health Services Research Program to study the evolution and impact of the project on EHR adoption.¹¹

Progress in Electronic Prescribing is presently being evaluated in the state of Nebraska to determine the progress being made as expected by federal legislation. Federal legislation entitled the Medicare Prescription Drug, Improvement and Modernization Act of 2003 established a requirement for an “e-prescribing Program”. Prescriptions and eligibility, formulary and drug safety information written and transmitted electronically for Medicare beneficiaries receiving covered Medicare drugs must conform to uniform standards established under this legislation no later than April 1, 2009. However, the Secretary HHS may require conformity sooner.¹² National research in 2005 revealed that e-prescribing of any form was only practiced by 15 percent of physicians. Problems such as a lack of unified standards and an uneven distribution of related costs are some of the reasons. It is also pointed out that the e-prescribing systems available may lack the advanced features needed to improve patient safety and chronic disease control.¹³ With the Medicare program adoption of the prescription drug benefit, some argue that the government should consider additional incentives to spur the uptake of more advanced systems.¹⁴

Two projects are underway that are assessing the progress in both medical practices and pharmacies. The first is the project described above through the Nebraska Medical Association and the Creighton Health Services Research Program.¹² The second is a project sponsored by the Nebraska State Board of Pharmacy through the Dyke Anderson Patient Safety Grant. An overview of this project is described in the report section entitled, “State Initiatives in Health Information Technology and Patient Safety”. Data about the state of progress is expected to be available in late 2007 or early 2008.

Consumer Perspectives

National perspectives of consumers about quality and safety are consistent with the state research findings about the sharing of personal health information. A 2006 report from The Commonwealth Fund Commission surveyed U.S. adults to determine the public's perspectives on ways to improve patient care and on health policy priorities facing the President and Congress. 42 percent of the more than 1,000 adults interviewed reported experiencing poorly coordinated, inefficient, or unsafe care at some time over the last two years. One of four U.S. adults reported that their physician had recommended unnecessary care or treatment, and one of six reported their physician ordered tests that already had been done. Poorly coordinated health care efforts are to blame. Overall, the representative sample of 1,023 adults ages 18 and older revealed strong public support for efforts to improve care coordination and access to information. Respondents support steps such as expanded use of information technology and physicians, nurses, and other health care practitioners working as a team to improve the quality of care. Patients reported recent experiences of wasteful, inefficient, or unsafe care. In addition, half of middle-income and lower-income families reported serious problems paying for care and insurance coverage. Three-quarters of all adults said the U.S. health care system needs either fundamental change or complete rebuilding. Expanding insurance and controlling costs, they said, should be top priorities for federal action.¹⁵

Serious medical errors continue to be common. These experiences shape consumer viewpoints about our health care system needs. The Commonwealth Fund survey on shaping the future of the U.S. Health System determined that adults who had experienced serious problems with their care are more likely to say the health care system needs to be completely rebuilt compared with those reporting no serious problems. Forty-three percent of those who had experienced a medical error in the past two years said the system needs to be rebuilt, compared with 27 percent of those who did not experience a medical error.¹⁵

Security and Privacy Issues

Security and privacy issues continue to be a primary area of need to be addressed nationally. Much of what we seem to be discovering is the need for unbiased information, lots of quality education, and a lot more research. National wide and federal initiatives have been intensely focused on security and the privacy concerns for the last two years. Key reports and guidance documents are being developed through these initiatives. One of these is the Connecting for Health Common Framework, developed by a public-private collaborative made up of more than 100 organizations. The Connecting for Health initiative is supported through the Markle Foundation (see website link in Appendix B: Learning Resources). The Connecting for Health steering committee published the “Achieving Connectivity in Healthcare: A Preliminary Roadmap from the Nation’s Public and Private Sector Healthcare Leaders”. This roadmap sketched a vision of nationwide health information exchange of decentralized networks united by a common framework of policies and standards that put patient privacy first.

A more recently nationally funded work through the Agency for Healthcare Research and Quality is the project entitled the Health Information Security and Privacy Collaboration (HISPC). This is a 33 state and one territory funded project that represents a cross-sectional look at the major areas states have identified as presenting challenges to the privacy and security of electronic health information exchange (HIE). An interim assessment of variation between organizational level business practices, policies and laws related to privacy and security are identified across the participating states and territory. This has been published as the “Privacy and Security Solutions for Interoperable

Health Information Exchange – Interim Assessment of Variation” report.¹⁶ To date, key points identified in this national cross-section study include:

- There is substantial variation in all three areas of study (business practices, policy and law) in this project
- Many business practice variations are attributed to different interpretations of the requirements of the HIPAA – particularly in the area of patient consent or authorization across organizations.
- Businesses view exchanging information as a potential liability – concerned about the varying quality of security systems between exchanging organizations.
- Trust was a concern expressed by providers who were concerned about liability from the activities of others who they sent data to and lawsuits from consumers for inappropriate disclosure.
- Trust was a concern expressed by consumers who were worried about privacy risks from the implementation of new technologies and the potential for unauthorized disclosures of sensitive information to payers and employers.
- There are misunderstandings about how state laws, HIPAA rules and regulations, and federal laws intersect.
- There is confusion about where state laws are found and how they should be applied.
- There is an absence of state laws clearly applicable to electronic health information exchange
- Direct conflicts exist with legislation related to substance abuse treatment and patient confidentiality, the practice of pharmacy involving electronic prescription data exchange, and Clinical Laboratory Improvement Amendments (CLIA) that defer to state law.
- States have an absence of regional eHIE networks, limited deployment of electronic health record systems, and lack of interoperability of the systems that have been deployed.
- Variation in patient record matching is high.
- Issues related to disclosure of personal health information are:
 - General lack of consistent and accurate understanding of federal and state laws with respect to disclosures
 - Issues surrounding the interpretation, requirement and use of patient consent or patient authorization in connection with the release of information
 - Issues related to the re-release or re-disclosure of information
 - HIPAA minimum necessary requirement
 - Ownership and control of health information
 - Differences in the way certain health information should be treated
 - Varying degrees of reporting requirements for public health purposes
 - Handling of disclosures related to judicial proceedings and law enforcement
 - Human judgment factor in determining disclosure
 - Acceptability of digital signatures to support patient consent and patient authorization

Our own state of Nebraska HISPC study of security and privacy issues has independently arrived at identification of the same concerns and areas of work needing to be addressed within our state and its’ communities. The national HISPC report may serve as a resource document to assist us as we move forward in our continued assessment and action plan within Nebraska. More resources are being generated through national efforts. In mid-June 2007, the Government Accountability Office (GAO) released a report indicating that although efforts are continuing, a comprehensive privacy approach is needed for a national strategy.¹⁷ Both our national and state level studies indicate that a sustainable method of tracking and monitoring actions and progress is needed within our state.

Findings and Recommendations

Finding 1: Facilitation of knowledge and understanding about health information exchange is essential for the Nebraska Health and Human Services Health Board managers and Facility Oversight Managers. This knowledge directly affects the management of security and privacy issues. Managers who are equipped with this understanding can assist the boards to address how current and future rules and regulations affect and are affected by the evolving landscape of health information exchange and interoperability.

Recommendation:

- **Nebraska Health and Human services develop a process for obtaining timely and up to date technical information on health information and interoperability and disseminating this to health/ licensure/ certification board managers and their members.**
- **Nebraska Health and Human services charge managers to facilitate the boards to address how current and future rules and regulations affect and are affected by the advancement of health information exchange and interoperability.**

Finding 2: Facilitation of knowledge and understanding of health professionals across the state is an important role that the health professions organizations can perform. These organizations vary in their engagement and understanding of the technical information about health information interoperability and the related security and privacy issues. The organizations would provide a great service in the process of informing their members about understanding health information exchange and interoperability, and the related security and privacy practices and issues.

Further, the unique knowledge and expertise of health care practitioners, facilities in which health care is provided, organizations involved with health issues at the societal level and educators of health professions students, is needed to address how current laws, rules and regulations related to their disciplines affect and are affected by the electronic exchange of health information. We encourage these associations to seek additional information about health information exchange and interoperability in other regions within the state, region, nationally and internationally.

Recommendation:

- **The e-Health Council engages all health professional associations involved in health care delivery and services to assist in present and future efforts to design, implement and educate key stakeholders in the health professions, health education and health organizations about the sharing of health information, and the related security and privacy issues as these processes unfold.**

Finding 3: The HISPC recognizes that state government, boards and health care providers need more knowledge about the Nebraska consumer. Consumer viewpoints are critical to this broader understanding of health information exchange and interoperability. A larger and broader representation of consumer viewpoints and needs will greatly improve our understanding of “what” consumers will participate in and “how” they will participate.

Similarly, consumers are in great need of information and education about health information exchange and interoperability. Consumers have concerns that must be addressed through knowledge dissemination. This will facilitate the best decision-making possible for the consumer. A dissemination process for essential and timely information related to progress of this initiative occurring at both the federal and state level to consumers is needed.

A variety of ways of consumer involvement are needed to assist in the design of the processes of education of all stakeholders and policy formulation as the macro system of sharing health information electronically unfolds over time. This is an essential step to facilitating citizens and providers to more easily establish a common understanding and agreed upon set of solutions to health information exchange as security and privacy issues are addressed.

Recommendation:

- **The e-Health Council engage consumers to assist in present and future efforts to design, implement and educate other consumers and key stakeholders in the health professions, health education and health organizations about the sharing of health information, and the related security and privacy issues as these processes unfold.**

Finding 4: The complexity of the rules and regulations create confusion in the area of privacy. Because the HIPAA preemption rules are complex, individuals in a position to potentially disclose protected health information (PHI) sometimes are unsure if the PHI may be disclosed without written individual authorization. Health care providers and payers who are faced with potential civil and criminal HIPAA fines and penalties, state law causes of action for invasion of privacy, and reporting to licensure boards for breach of confidentiality, may often decide not to disclose PHI without written patient authorization, when it is otherwise permissible to disclose.

Recommendation:

- **The e-Health Council should study the issues identified and described in the background information of this report and recommend a sustainable action plan developed to facilitate progress in assuring privacy and security protections of the individual while progressing in health information exchange.**

Finding 5: Our HISPC study of security and privacy issues is consistent with the same concerns and areas of work needing to be addressed within our state and its' communities as a most recent cross-sectional study of the nation revealed.¹ The issues are embedded in complexity and confusion associated with state and federal level inconsistencies, conflicting business practices, and varying consent policies and approaches. These issues must be untangled and addressed. This will require a sustained commitment to achieve.

¹ 16. Dimitropoulos, L.L. Interim assessment of variation: privacy and security solutions for interoperable health information exchange. December 29, 2006. RTI Project No. 0209825.000.004.002. RTI International, Chicago, Illinois.

Recommendation:

- **The e-Health Council should explore the development of a sustainable system for monitoring our progress in studying and addressing the security and privacy issues within the state of Nebraska.**
- **An in-depth study of existing laws and regulations, with guidance from representatives from health professions, health educators and health organizations is needed to develop solutions on how to overcome these barriers.**

Finding 6: Based on the three research reports from this committee and our discussions, we believe there is a need for further research needed about implications to consumers, health professionals, health systems, educators, private and public care providers, and payers. Examples of important research questions that the committee has thought about, but are not limited to include:

- How are consumer's health and safety outcomes affected by the sharing of health information?
- What processes are necessary for consumers to participate in the sharing of health information?
- How will consumers concerns about the risks they perceive with health information sharing be "stewarded" as the processes emerge, and who will "steward" them?
- How are small business health care providers, health systems and large healthcare organizations, affected by the impact of sharing health information: What is the impact on workload? What is the impact on workforce considerations?
- How will the educational needs of the young, middle age, young-old and old-old adults be met as these processes develop?
- What is the impact of a partial adoption of health information sharing on patient security and privacy?

Recommendation:

- **The NHHS should pursue further research in the area of how to obtain needed technical information and employ effective processes of applying this information to assist health boards and facility boards with the ongoing process of staying current in and facilitating adoption of future rules and regulations that advance secure, private health information and interoperability approaches.**
- **Further research should be conducted by professional organizations about the on-going impact of health information and exchange and interoperability on provider and patient security and privacy issues.**
- **Further research should be conducted to better understand consumer viewpoints and needs.**

References

1. Berens, D., Galt, K.A., and HISPC Committee. *Report 1: Survey of Health/Licensure/Certification and Facilities Oversight Board Managers, 2007*. <http://chrp.creighton.edu>. Accessed: June 19, 2007.
2. Berens, D., Galt, K.A., and HISPC Committee. *Report 2: Survey of Health Professions Organizations Leadership, 2007*. <http://chrp.creighton.edu>. Accessed: June 19, 2007.
3. Berens, D., Galt, K.A., Paschal, K., and HISPC Committee. *Report 3: Study of Consumer View Points on Health Information, Security, and Privacy, 2007*. <http://chrp.creighton.edu>. Accessed: June 19, 2007.
4. Baird, Holm, McEachen, Pedersen, Hamann & Strasheim, LLP. *NHA: Updated HIPAA Preemption Analysis for Providers*. Nebraska Hospital Association, April 15, 2003.
5. John Woolley and Gerhard Peters, Executive Order 13410 - Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs August 22nd, 2006. *The American Presidency Project* [online]. Santa Barbara, CA: University of California (hosted), Gerhard Peters (database). Available from World Wide Web: (<http://www.presidency.ucsb.edu/ws/?pid=605>).
6. Dresden, D. *Keeping Secrets in Pharmacy*. *PharmacyWeek*, 2006;15(43):5.
7. Institute of Medicine. *To Err is Human: Building a Safer Health System*. Washington, DC: National Academy Press, 1999. <http://www.nap.edu>. Accessed: January 2000.
8. Anon. *The Kaiser Family Foundation/Agency for Healthcare Research and Quality/Harvard School of Public Health National Survey on Consumers' Experiences With Patient Safety and Quality Information, November 2004*. <http://kff.org/kaiserpolls/7210.cfm>. Accessed: June 19, 2007.
9. Nolan, K. Briefing on the State Alliance for e-Health. Presentation January 2007. http://www.hhs.gov/healthit/ahic/materials/01_07/bio/Nolan.ppt. Accessed: June 21, 2007.
10. Jha, A.K., Ferris, T.G., Donelan, K., DesRoches, C., Shields, A., Rosenbaum, S., Blumenthal, D. *How Common Are Electronic Health Records In The United States? A Summary Of The Evidence*. *Health Aff (Millwood)*. 2006 Nov-Dec;25(6):w496-507.
11. Galt, K.A., Johnson, S., and the EHRNebraska Research Team: Abbott, A., Anderson, D., Bramble, J.D., Drincic, A., Fuji, K.T., Glover, D., Kasha, T., Mahlman, D., Paschal, K., Siracuse, M., Rule, A. *How Many Physician Practices Have Adopted Electronic Health Records in Nebraska? An Update on the Nebraska Medical Association EHRNebraska Project*. (June 2007; in press, the Nebraska Medical Association). <http://chrp.creighton.edu>. Accessed June 20, 2007.
12. Adapted from: *Electronic Prescribing: Towards Maximum Value and Rapid Adoption, eHealth Initiative, 2004*. <http://www.ehealthinitiative.org/> Accessed: September 2006.

13. Sasrasohn-Kahn, J., Holt, M. *The Prescription Infrastructure: Are We Ready for ePrescribing?* California Healthcare Foundation, January 2006. <http://www.chcf.org>. Accessed: August 2006.
14. Bell, D.S., Friedman, M.A. *E-prescribing and the medicare modernization act of 2003. Paving the on-ramp to fully integrated health information technology?* Health Aff (Millwood). 2005 Sep-Oct;24(5):1159-69.
15. Schoen, C., How, S.K.H, Weinbaum, I., Craig, Jr., J.E., and Davis, K. *Public Views on Shaping the Future of the U.S. Health System*, The Commonwealth Fund, August 2006. <http://www.cmwf.org>. Accessed: January 2007.
16. Dimitropoulos, L.L. *Interim assessment of variation: privacy and security solutions for interoperable health information exchange*. December 29, 2006. RTI Project No. 0209825.000.004.002. RTI International, Chicago, Illinois.
17. Koontz, L.D., Melvin, V.C. Testimony Before the Subcommittee on Information Policy, Census, and National Archives Committee on Oversight and Government Reform U.S. House of Representatives. *Health Information Technology: Efforts Continue but Comprehensive Privacy Approach Needed for National Strategy*. Document No. GAO-07-988T. www.gao.gov/cgi-bin/getrpt?GAO-07-988T. Accessed: June 20, 2007.

Appendix A

Nebraska Information Technology Commission **eHealth Council Charter**

1. Introduction

The eHealth Council (hereafter referred to as “Council”) of the Nebraska Information Technology Commission (hereafter referred to as “Commission”) is an advisory committee of the Commission composed of representatives from the State of Nebraska and federal government; health care providers; eHealth initiatives; public health; payers and employers; consumers; and resource providers. The Council was originally formed by the Nebraska Information Technology Commission on Feb. 22, 2007 to foster the collaborative and innovative use of eHealth technologies through partnerships between public and private sectors, and to encourage communication and coordination among eHealth initiatives in Nebraska.

2. Purpose

The purpose of this Charter is to clarify the role of the Council and its relationship with the Commission.

3. Authority

The Nebraska Information Technology Commission shall: "Establish ad hoc technical advisory groups to study and make recommendations on specific topics, including work groups to establish, coordinate, and prioritize needs for education, local communities, and state agencies[.]" Neb. Rev. Stat. § 86-516(7).

4. Commission Responsibilities and Mission

4.1 Commission Mission

The mission of the Nebraska Information Technology Commission is to make the State of Nebraska's investment in information technology infrastructure more accessible and responsive to the needs of its citizens regardless of location while making government, education, health care and other services more efficient and cost effective.

4.2 Commission Responsibilities (Neb. Rev. Stat. § 86-516)

4.2.1 Annually by July 1, adopt policies and procedures used to develop, review, and annually update a statewide technology plan;

4.2.2 Create an information technology clearinghouse to identify and share best practices and new developments, as well as identify existing problems and deficiencies;

4.2.3 Review and adopt policies to provide incentives for investments in information technology infrastructure services;

4.2.4 Determine a broad strategy and objectives for developing and sustaining information technology development in Nebraska, including long-range funding strategies, research and development investment, support and maintenance requirements, and system usage and assessment guidelines;

4.2.5 Adopt guidelines regarding project planning and management, information sharing, and administrative and technical review procedures involving state-owned or state-supported technology and infrastructure. Governmental entities, state agencies, and political subdivisions shall submit projects which directly utilize state-appropriated funds for information technology purposes to the process established by sections 86-512 to 86-524. Governmental entities and political subdivisions may submit other projects involving information technology to the commission for comment, review, and recommendations;

4.2.6 Adopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel;

4.2.7 Establish ad hoc technical advisory groups to study and make recommendations on specific topics, including workgroups to establish, coordinate, and prioritize needs for education, local communities, and state agencies;

4.2.8 By November 15 of each even-numbered year, make recommendations on technology investments to the Governor and the Legislature, including a prioritized list of projects, reviewed by the technical panel, for which new or additional funding is requested;

4.2.9 Approve grants from the Community Technology Fund and Government Technology Collaboration Fund;

4.2.10 Adopt schedules and procedures for reporting needs, priorities, and recommended projects ;
and

4.2.11 Assist the Chief Information Officer in developing and maintaining Network Nebraska pursuant to section 86-5,100.

5. eHealth Council Mission and Responsibilities

5.1 Council Mission

The mission of the Council is to foster the collaborative and innovative use of eHealth technologies through partnerships between public and private sectors, and to encourage communication and coordination among eHealth initiatives in Nebraska.

5.2 Council Responsibilities

5.2.1 Assist the Commission in developing, reviewing and updating the statewide technology plan.

5.2.2 Review the current status of healthcare information technology adoption by the healthcare delivery system in Nebraska;

5.2.3 Address potential security, privacy and other issues related to the adoption of interoperable healthcare information technology in Nebraska;

5.2.4 Evaluate the cost of using interoperable healthcare information technology by the healthcare delivery system in Nebraska;

5.2.5 Identify private resources and public/private partnerships to fund efforts to adopt interoperable healthcare information technology;

5.2.6 Support and promote the use of telehealth as a vehicle to improve healthcare access to Nebraskans;

5.2.7 Recommend best practices or policies for state government and private entities to promote the adoption of interoperable healthcare information technology by the healthcare delivery system in Nebraska.

6. Membership

6.1 Selection of Members

The Commission may solicit nominations from organizations or individuals with an active interest or involvement in eHealth in forming the initial set of members.

The Commission may also seek out additional qualified candidates. Nominations shall describe the qualifications of the person relative to the goals of the eHealth Council. In choosing members, the eHealth Council and the NITC shall strive for a balance of perspectives on eHealth issues.

6.2 Representation

The following focus areas will be represented within the eHealth Council:

6.2.1 The State of Nebraska

6.2.2 Health care providers

6.2.3 eHealth initiatives

6.2.4 Public health

6.2.4 Third party payers and employers

6.2.5 Consumers

6.2.6 Resource providers, experts, and others if deemed appropriate by the NITC

6.3 Number of Members

The number of members shall be no more than 25.

6.4 Vacancies

The eHealth Council may solicit nominations to fill vacant positions and may recommend new members to the NITC for approval. The Commission may also seek out additional qualified candidates.

6.5 Length of Service

One-third of the members shall initially serve 3-year terms. One-third of members will initially serve two-year terms. One-third of members will initially serve one-year terms. Subsequent terms will be three-years. Elected officials will serve as ex-officio members and will be appointed annually by the NITC.

6.6 Member Responsibilities

Each member is responsible for maintaining two-way communication with their sector constituents concerning issues brought before the Council.

6.7 Designated Alternates and Non-voting Alternates

6.7.1 Each member of the Council may designate one (1) official voting alternate. This official voting alternate shall be registered with the Office of the Chief Information Officer and NITC and, in the absence of the official member, have all the privileges as the official member on items of discussion and voting.

6.7.2 If the official member and his/her official alternate are unable to attend a Council meeting either in person or electronically, then the sub-sector affected may send a non-voting alternate to gather or share information.

7. Meeting Procedures

7.1 Chair(s)

The elected Chair or Co-Chairs will conduct the meetings of the Council, oversee the establishment, operation and dissolution of committees, propose meeting agendas, and maintain the general operations of the Council. The Chair or Co-Chairs of the Council will serve two year staggered terms, expiring on January 1. If co-chairs are selected initially, one co-chair will serve two years, and one will serve three years. Subsequent co-chairs shall serve 2-year terms.

7.2 Quorum

An official quorum consists of 50% of the official members or their voting alternates. No official voting business may be conducted without an official quorum.

7.3 Voting

Issues shall be decided by a majority vote of the voting members present.

7.4 Meeting Frequency

The Council shall meet on an as needed basis. The eHealth Council will meet no more than 8 and no fewer than 2 times per year.

7.5 Notice of Meetings

7.5.1 Notice of the time and place of each meeting of the Council shall be made at least seven (7) calendar days prior to the meeting. Notice shall be published on the Council's Web site at <http://www.nitc.state.ne.us/>.

7.5.2 The notice shall contain an agenda of subjects known at the time of the publicized notice or a statement that the agenda shall be readily available for public inspection at the Office of the Chief Information Officer, 501 S. 14th Street, 4th Floor, Lincoln, NE, during normal business hours by appointment.

7.6 Subcommittees

7.6.1 Subcommittees will be designated by vote of the Council to address specific topics.

7.6.2 Pursuant to provisions of Neb. Rev. Stat. § 84-1409(1), subcommittees of the Council shall not be required to provide notice of meetings.

7.7 Expense Reimbursement

Section 81-1182.01 states: "Any department, agency, commission, council, committee, or board of the state may pay for the reasonable and necessary expenses for the recruitment, training, utilization, and recognition of volunteers providing services to the state and certain providers of services as established by the Director of Administrative Services."

7.7.1 According to NAS Policy CONC-005, "Volunteers shall mean those persons providing services to the State who are not being compensated for their time."

7.7.2 Council members needing reimbursement must submit a signed request to the Office of the CIO-NITC using the official state accounting forms.

Appendix B

Nebraska Initiatives in Health Information Technology and Patient Safety

Policy and Coordination

- **Nebraska Information Technology Commission eHealth Council.** The NITC created an eHealth Council to facilitate discussions among eHealth initiatives and to make recommendations to the NITC regarding the adoption and interoperability of eHealth technologies on Feb. 22, 2007. The twenty-five member eHealth Council met for the first time on May 22, 2007. The eHealth Council is developing an eHealth Clearinghouse to facilitate the exchange of information on eHealth.

Regional Health Information Organization Initiatives (RHIOs) Initiatives

- **Western Nebraska Health Information Exchange.** Partners in Western Nebraska have completed a plan and are beginning to implement a regional health information exchange. Partial funding has been provided through an AHRQ planning grant, an AHRQ implementation grant, and a HRSA Rural Network Development grant.
- **Nebraska Health Information Initiative (NeHII).** The Nebraska Health Information Initiative (NeHII) is a collaboration of Nebraska health care organizations, hospitals, physicians, Blue Cross and Blue Shield of Nebraska, and the University of Nebraska Medical Center. The mission of the NeHII Collaborative is to provide Nebraska a system for the secure exchange and use of health information. NeHII is raising funds for start-up operations.
- **Southeast Nebraska Behavioral Health Information Network.** A \$200,000 one-year planning grant from the U.S. Department of Health and Human Services Agency for Healthcare Research and Quality (AHRQ) in 2004 enabled Region V Behavioral Health Care Providers to develop a plan to develop a health information technology infrastructure that will result in standards-based data sharing and lead to measurable and sustainable improvements in patient safety and quality of care in the region. Since the completion of the planning grant, SNBHIN partners have continued to meet and are making progress toward establishing a RHIO.

Electronic Medical, Health, and Personal Health Record Initiatives (EMR/EHR/PHR)

- **Nebraska Medical Association Project.** The Nebraska Medical Association Foundation received a two-year grant for \$499,604 from the Physicians Foundation for Health Systems Excellence to work with small and medium-sized physician practices on electronic health records and chronic disease management registries.
- **UNMC Web-based Personal Health Record.** The University of Nebraska Medical Center is establishing a Web-based Personal Health Record (PHR) program for all its students. In contrast with medical records that are owned by doctors or hospitals, a PHR is owned by the patient and is part of a national effort to involve patients in their own health care.

- **The Rural Comprehensive Care Network of Nebraska.** The Rural Comprehensive Care Network of Nebraska received a three-year grant from the U.S. Department of Health and Human Services Health Resources and Services Administration’s Rural Health Network Development Program in 2006. The grant will help physicians, hospitals, and pharmacies in the network communicate via electronic health records.
- **Nebraska Registry Partnership.** The project is a partnership of the Nebraska Office of Rural Health, Diabetes Prevention and Control Program—HHSS, Cardiovascular Health Program—HHSS, CIMRO of Nebraska, Nebraska Rural Health Association, and the University of Nebraska Medical Center. Through the project, DocSite implementation in pilot clinics has been completed.

Telehealth

- **Nebraska Statewide Telehealth Network.** The Nebraska Statewide Telehealth Network is an interactive video and data network that provides integration among all of the not for profit hospitals and public health departments in the state. The Nebraska Statewide Telehealth Network is unrivaled in scope by any other state telehealth network.

Privacy and Security

- **HISPC Steering Committee.** With funding from an AHRQ grant, researchers at the Creighton Health Services Research Program are involved in survey research to inform the HISPC Committee about security and privacy issues from different stakeholders in the state. (Berens, D. State Office of Rural Health Grant no. H95RH00119, Health Resource and Services Administration)

HIT Related Grants Received in Nebraska

Regional Health Information Organization Projects

- **HIT Plan for Region V Behavioral Health Care Providers (P20 HS15039)**
Institution: Heartland Health Alliance (Holbrook)
Investigator: Wende Baker
Objective: Plan and implement a methodology for behavioral health care providers to standardize core shared data elements; design an integrated management information system for sharing data; connect rural with urban providers; and develop messaging capabilities between primary and behavioral health care providers.
Sponsor: Agency for Healthcare Research and Quality (AHRQ)
- **Western Nebraska Health Information Exchange (P20 HS15365)**
Institution: Chadron Community Hospital (Lincoln)
Investigator: Nancy Shank
Objective: Plan the implementation of a regional health record system within established networks of rural hospitals, clinics, public health providers, behavioral health care providers, and others across a remote area covering 14,000 square mi.
Sponsor: Agency for Healthcare Research and Quality (AHRQ)

Patient Safety and Health Information Technology Projects

- **Medication Safety and Electronic Prescribing - Personal Digital Assistant Devices and Medication Error (R18 HS11808)**
Institution: Creighton University (Omaha) – Creighton Health Services Research Program
Investigator: Kimberly Galt
Objective: Determine the impact of prescriber use of personal digital assistant (PDA) technology on potential medication errors in primary care physician office-based practices and identify barriers to PDA use.
Sponsor: Agency for Healthcare Research and Quality (AHRQ)
- **The Creighton Health Services Research Program (CHRP) Development Grant – an AHRQ Building Research Infrastructure Capacity (BRIC) Program (1P20 HS015816)**
Institution: Creighton University (Omaha) - Creighton Health Services Research Program
Investigator: Kimberly Galt
Project: Redesigning a Model of HIT Adoption to Fit Error Reduction in Office-Based Physician
Objective: The BRIC program is a merit-based, peer-reviewed program in response to Congressional intent to broaden geographic distribution of health services research funding among institutions located in states in which the collective success rate for applications to the AHRQ have historically been low. The health services research grant will help Creighton University achieve and sustain long-term competitive funding while improving capacity and support for the research faculty as well as developing processes that support forming and maintaining interdisciplinary research teams and support timely dissemination of research products generated through the conduct of health services research. The emphasis is on Patient Safety and Health Information Technology.
Sponsor: Agency for Healthcare Research and Quality (AHRQ)
- **Implementing a Program of Patient Safety in Small Rural Hospitals (U18 HS15822)**
Institution: University of Nebraska Medical Center (Omaha)
Investigator: Katherine Jones, P.T.
Objective: Using a collaboration between an academic medical center and small rural hospitals, implement a voluntary program of medication error reporting, feedback, analysis, and system change.
Sponsor: Agency for Healthcare Research and Quality (AHRQ)
- **Patient Safety Improvement Corps**
Institution: CIMRO of Nebraska (QIO) (Lincoln)
Investigator: Greg Schieke
Partner: Fremont Area Medical Center
Project: The Heart of Safe Care at Fremont Area Medical Center
Objective: Increase knowledge and skill in patient safety practices; improve the safety environment through a comprehensive program designed to identify, evaluate, and prevent errors; develop projects that increase patient involvement in the patient safety process; restructure the error reporting system; encourage development of organizational learning about errors; and promote a culture of knowledge sharing.
Sponsor: Agency for Healthcare Research and Quality (AHRQ)

- **Dyke Anderson Patient Safety Grant**

Institution: Creighton University (Omaha) - Creighton Health Services Research Program

Investigator: Kimberly Galt

Project: Pharmacists for Patient Safety

Objective: This project will implement a patient safety program for pharmacists in all practice settings entitled, "*Pharmacists For Patient Safety*". The program will implement a voluntary error reporting process for pharmacists, analyze the reports for common and newly emerging errors, identify known prevention strategies to these errors that can be implemented in practice, provide education to pharmacists about these errors and how to implement prevention strategies in practice, and assess the impact of this error analysis and education program on actual implementation of safety practices by pharmacists in the state. The project is intended to reach and educate all pharmacists in the state in all practice settings. An assessment of new technologies, use of e-prescribing, and innovative methods to improve patient safety will be explored.

Sponsor: Nebraska HHS – State Board of Pharmacy

Appendix C

Health Information Technology Certification Resources

Health IT Certification

- <http://www.healthitcertification.com/overview.html>
- The designation of Certified Professional in Health Information Technology (CPHIT) indicates that the holder has mastered the common body of knowledge covering planning, selecting, implementing, using, and managing health information technology (HIT) and electronic health record (EHR) applications. The CPHIT curriculum introduces the use of health information technology in any setting within the continuum of care.
- The designation of Certified Professional in Electronic Health Records (CPEHR) indicates that the holder has mastered the common body of knowledge covering planning, implementation, and operation of EHR for knowledge management, quality improvement, patient safety, and care coordination. The CPEHR curriculum adjusts the strategies to make the most of an EHR investment, enhancing capabilities, using new technologies, and building value.

International Association of Privacy Professionals (IAPP) Privacy Certification

- <https://www.privacyassociation.org/>
- IAPP is the first organization to develop and launch quality credentialing programs that serve introductory to advanced courses for U.S. government and international privacy professionals.
- The Certified Information Privacy Professional (CIPP) is an essential foundation course for any privacy professional working in the field today or entering the field for the first time. The CIPP addresses the fundamentals of privacy law, technology, operations and information management. It is the industry's first broad-based certification and is made possible through founding grants from Hewlett-Packard Company and Microsoft Corporation.
- The IAPP also offers the first publicly available certification for U.S. government privacy professionals. The Certified Information Privacy Professional/Government (CIPP/G) is an extension of the CIPP certification and is designed exclusively for employees of U.S. federal government agencies as well as employees of state, county and local governments. The CIPP/G is made possible through the generous support of IBM.

General Learning Resources

American Health Information Management Association (AHIMA)

- <http://www.ahima.org/>

Agency for Healthcare Research and Quality

- www.ahrq.gov

California Healthcare Foundation

- www.chcf.org

Certification Commission for Healthcare Information Technology (CCHIT)

- <http://www.cchit.org/>
- CCHIT is a recognized certification body (RCB) for electronic health records and their networks, and an independent, voluntary, private-sector initiative.

Commonwealth Fund

- www.cmwf.org

Creighton Health Services Research Program

- www.chrp.creighton.edu

eHealth Initiative

- www.ehealthinitiative.org

Health Level Seven

- www.HL7.org

Markle Foundation - The Connecting for Health Common Framework Project

- www.markle.org
- http://www.markle.org/markle_programs/healthcare/projects/connecting_for_health.php

National Council for Prescription Drug Programs

- www.ncdp.org

National Governors Association

- <http://www.nga.org/portal/site/nga>

Nebraska CIMRO

- www.cimronebraska.org

Nebraska HHS System Office of Rural Health

- www.hhs.state.ne.us/orh/

Nebraska Information Technology Commission

- www.nitc.state.ne.us/

Office of the National Coordinator for Health Information Technology (ONC or ONCHIT)

- <http://www.hhs.gov/healthit/rfi.html>

Vanderbilt Center for Better Health

- www.mc.vanderbilt.edu/vcbh/

U.S. Department of Labor

Employee Benefits Security Administration

Report Of The Working Group On Health Information Technology

- www.dol.gov/ebsa

Nebraska Health Professions Related Associations

Lancaster County Medical Society
www.countymedicalsociety.org

Metro Omaha Medical Society
<http://www.omahamedical.com>
National Association of Social Workers Nebraska Chapter
www.naswne.org

National Funeral Directors Association
www.nfda.org

Nebraska Academy of Family Physicians
www.nebrafp.org

Nebraska Chiropractic Physicians Association
www.nechiropractic.org

Nebraska Dental Association
www.nedental.org

Nebraska Dietetic Association
www.eatrightnebraska.org

Nebraska Emergency Medical Services Association
www.nemsa.org

Nebraska Emergency Nurses Association
www.enanebraska.org

Nebraska Environmental Health Association
www.nebraskaneha.org

Nebraska Funeral Directors Association
www.nefda.org

Nebraska Health Care Association - Nebraska Assisted Living Association
www.nehca.org

Nebraska Hearing Society
www.nebraskahearingsociety.org

Nebraska Hospice & Palliative Care Association
www.nebraskahospice.org

Nebraska Hospital Association
www.nhanet.org

Nebraska Medical Association

www.nebmed.org

Nebraska Mental Health Association

www.mha-ne.org

Nebraska Minority Public Health Association

www.nempha.org

Nebraska Nurses Association

www.nursingworld.org

Nebraska Occupational Therapy Association

www.notaonline.org

Nebraska Optometric Association

www.noaonline.org

Nebraska Pharmacists Association

<http://www.npharm.org>

Nebraska Physical Therapy Association

<http://www.npta.org>

Nebraska Podiatric Medical Association

<http://nefootandankle.org/>

Nebraska Psychological Association

<http://www.nebpsych.org>

Nebraska Society for Respiratory Care

www.nsrc-online.org

Nebraska Speech-Language-Hearing Association

www.nslha.org

Nebraska Veterinary Medical Association

<http://www.nvma.org>

Public Health Association of Nebraska

www.publichealthne.org

Rural Comprehensive Care Network

<http://www.rccn.info>

South East Rural Physicians Alliance

<http://www.serpa-ne.org>

Appendix D

Taxonomy for Health Care and Information Technology Professionals

The language used in the health information technology literature and conversations can be specific and unique. The following taxonomy and definitions is provided as a resource to assist us in achieving a common understanding. These definitions are compiled from multiple sources. Many have been taken from the <http://toolkits.ehealthinitiative.org/glossary/> Accessed May 30, 2007. The contents of eHI's *Connecting Communities Toolkit* are licensed under a [Creative Commons Attribution-ShareAlike 2.5 License](http://creativecommons.org/licenses/by-sa/2.5/) (<http://creativecommons.org/licenses/by-sa/2.5/> License for *Connecting Communities Toolkit*). As health information exchange advances, new terms and revisions to existing terms are likely. This listing provides a basic introduction as we currently understand this area.

Access:

The process of obtaining data from, or placing into a computer system or storage device. It refers to such actions by any individual or entity who has the appropriate authorization for such actions.

Active Conditions/Diagnoses:

Information maintained in the patient record related to medical conditions or current diagnosed diseases.

Active Medications:

Medications a patient is currently taking. These include prescription medications, over the counter substances, nutritional supplements, natural products and alternative medicines.

AHRQ:

Agency for Healthcare Research Quality, a part of the U.S. Department of Health and Human Services.

Ambulatory Surgical Centers:

Ambulatory surgery centers (ASCs) are medical facilities that specialize in elective same-day or outpatient surgical procedures. They do not offer emergency care.

American National Standards Institute (ANSI):

ANSI is a broad based agency charged with overseeing voluntary standards development for everything from computers to household products. ANSI accredits standards development organizations (SDO) based on their consensus process, then reviews and officially approves the SDO recommendations.

American Society for Testing and Materials (ASTM):

American Society for Testing and Materials develops standards on characteristics and performance of materials, products, systems, and services. There are numerous standards-writing technical committees. E31 is the Committee on Computerized Systems and E31.28 is the subcommittee on Healthcare Informatics responsible for the Continuity of Care (CCR) standard.

Application Service Provider (ASP):

An ASP is a company that creates health (and in many other arenas, as well) information technology solutions available on a subscription basis to health care entities and RHIOS. The ASP distributes

the solution from its home central location to customers elsewhere. Thus, an ASP is responsible for maintaining, updating, and troubleshooting solutions (making sure it is available 24/7, ensuring redundancy, etc) that health care entities/RHIOs would otherwise be responsible for doing. ASPs can be an inexpensive way to manage information services.

Architecture:

A formal description of an IT system. There are three general architectural approaches being used in health information exchange:

Centralized architecture Data sharing and inter-change of electronic information emphasizing full control over data sharing through a centralized repository. Components in a centralized architecture refer to the Central Data Repository (CDR) and the requestor. The CDR authenticates the requestor through a technological means, authorizes the transaction and records it for audit and reporting purposes.

Federated architecture Independent databases (decentralized) are connected to share and exchange information. The federated architecture provides a means to share data and transactions using messaging services, combine information from several components and coordinate activities among autonomous components.

P2P (peer-to-peer): A general term for popular file-sharing systems in which there is no central repository of files. Files can be stored on and retrieved from any user's computer.

Asymmetric Key System:

A system that uses different keys for encryption and decryption. Within such a system, it is computationally infeasible to determine the decryption key (which is kept private) from the encryption key (which is made publicly available).

Audit trail:

Chronological record of system activity which enables the reconstruction of information regarding the creation, distribution, modification, and deletion of data.

Authentication:

A method to verify that the person or entity seeking access to information on a secured Health Information Exchange is the one claimed.

Authorization:

The role or set of permissions for information system activity assigned to an individual.

Biometric Authentication Technology:

Technology that uses some human biological feature (e.g. fingerprint, voice pattern, retina scan, or signature dynamics) to uniquely identify an individual.

Certification/Conformance Testing:

Testing a product for the existence of specific features, functions, or characteristics required by a standard in order to determine the extent to which that product satisfies the standard requirements.

Clinical Data Repository:

Clinical database optimized for storage and retrieval of information on individual patients and used to support patient care and daily operations.

Chart Review:

The retrospective review of the patient's complete written record by an expert for the purpose of a specific analysis. For patient safety, to identify possible adverse events by reviewing the physician and nursing progress notes and careful examination for certain indicators.

Chief Complaint Mapper:

A software product that maps chief complaints, captured as text, and transforms them into useful digital data that can be used in functions such as public health outbreak surveillance.

Clinical Classification:

A method of grouping clinical concepts in order to represent classes that support the generation of indicators of health status and health statistics.

Clinical Data Repository:

The data warehouse that contains clinical data (HL7 messages) centrally.

Clinical Messaging:

The communication among providers involved in the care process that can range from real time communication (for example, fulfillment of an injection while the patient is in the exam room), to asynchronous communication (for example, consult reports between physicians).

Clinical Messaging #1:

Continuity of Care Data Exchanges (Inter-Provider Communication): Communication among providers involved in the care process can range from real time communication (for example, fulfillment of an injection while the patient is in the exam room), to asynchronous communication (for example, consult reports between physicians). Some forms of inter-practitioner communication will be paper based and the EHRS must be able to produce appropriate documents.

Clinical Messaging #2:

Secure Patient/Physician e-mail (Provider and Patient or Family Communication): Trigger or respond to electronic communication (inbound and outbound) between providers and patients or patient representatives with pertinent actions in the care process.

Clinical records:

A chronological written account of a patient's examination and treatment that includes the patient's medical history and complaints, the physician's physical findings, the results of diagnostic tests and procedures, and medications and therapeutic procedures.

Clinical Reminders (Clinical Guideline Prompts):

The ability to remind clinicians to consider certain actions at a particular point in time, such as prompts to ask the patient appropriate preventive medicine questions, notifications that ordered tests have not produced results when expected, and suggestions for certain therapeutic actions, such as giving a tetanus shot if one has not been given for 10 years.

Computerized Provider Order Entry (CPOE):

A computer application that allows a physician's orders for diagnostic and treatment services (such as medications, laboratory, and other tests) to be entered electronically instead of being recorded on order sheets or prescription pads. The computer compares the order against standards for dosing, checks for allergies or interactions with other medications, and warns the physician about potential problems.

Confidentiality:

A 3rd party's obligation to protect the personal information with which it has been entrusted.

Continuity of Care Record:

A core dataset to be sent to the next healthcare provider whenever a patient is referred, transferred, or otherwise uses different clinics, hospitals, or other providers. The CCR will provide the necessary information to support continuity of care. The ASTM CCR is a patient health summary standard, a way to create flexible documents that contain the most relevant and timely core clinical information about a patient, and to send these electronically from one care giver to another or to provide them directly to patients. An ASTM International standard, the standard, E 2369, Specification for Continuity of Care Record (CCR), was developed by Subcommittee E31.28 on Electronic Health Records, which is under the jurisdiction of Committee E31 on Healthcare Informatics.

Controlled Clinical Vocabulary:

A system of standardizing the terms used in describing client-centered health and health service-related concepts.

Data Center:

The physical space and hardware used by the HIE to house its operations if these assets are kept within the HIE.

Data Integrity:

The accuracy and completeness of data, to be maintained by appropriate security measures and controls. Preservation of the original quality and accuracy of data, in written or in electronic form.

Data Recovery Services:

A mechanism and process to safely store duplicate databases and recreate the data should a disaster occur.

Data security:

The process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption.

Decision Support:

Computerized functions that assist users in making decisions in their job functions. In the practice of medicine, these functions include providing electronic access to medical literature, alerting the user to potential adverse drug interactions, and suggesting alternative treatment plans for a certain diagnosis.

Decryption:

The technique of using mathematical procedures to "unscramble" data so that an unintelligible (encrypted) message becomes intelligible.

DICOM (Digital Imaging Communications in Medicine):

A standard which defines protocols for the exchange of medical images and associated information (such as patient identification details and technique information) between instruments, information systems, and health care providers. It establishes a common language that enables medical images produced on one system to be processed and displayed on another.

Digital Signature:

A string of binary digits which is computed using an encryption algorithm. Digital signatures enable signatory authentication, confirmation of data integrity, and non-repudiation of messages.

Doctor Matching:

The process of cross-linking the multiple provider identifiers in a community from a variety of provider identifier sources and creating a master doctor identifier with a key for cross-referencing the various community identifiers.

Document Review, Edit, Sign:

A software process that allows for the secure review, editing, and signature through electronic, distributed technology of electronic health record components, such as operative reports, discharge summaries, and consultations.

e-Laboratory:

The electronic delivery of laboratory results to practices so that such data may be integrated into electronic patient records in a full EHR system, or used by a dedicated application to view structured, context-rich, and/or longitudinal laboratory results on a patient.

Electronic Billing Support:

The ability to contact the payer before the patient is seen and get a response that indicates whether or not the services to be rendered will be covered by the payer.

Electronic health records:

Extends the notion of an EMR to include the concept of cross-institutional data sharing. Thus, an EHR contains data from a subset of each institution's EMR (that is agreed upon by the institution). An EHR may also reside "entirely within one institution" and link the various affiliated practice sites together. The EHR is generally patient focused and spans episodes of care rather than a single encounter. An EHR can only be present if the participating sites all have an EMR in place that is interoperable.

Electronic Imaging Results Delivery:

The ability to accept messages from radiology sources and integrate the data for presentation to a clinician.

Electronic medical record (EMR):

The set of databases (or repositories) that contains the health information for patients within a given institution or organization. Thus, an EMR contains the aggregated datasets gathered from a variety of clinical service delivery processes, including laboratory data, pharmacy data, patient registration data, radiology data, surgical procedures, clinic and inpatient notes, preventive care delivery, emergency department visits, billing information, and others. EMRs may contain clinical applications that can act on the data contained within this repository; e.g., a clinical decision support system (CDSS), a computerized provider order entry system (CPOE), a controlled medical vocabulary, or a results-reporting system.

Electronic Prescribing (e-Prescribing):

Electronic prescription (e-prescribing) writing is defined by the eHealth Initiative as "the use of computing devices to enter, modify, review, and output or communicate drug prescriptions." Although the term e-prescribing implies the use of a computer for any type of prescribing action, there are a wide range of e-prescribing activities with varying levels of sophistication:

Level 1 - electronic reference handbook

Level 2 - standalone prescription writer

Level 3 - patient-specific prescription creation or refilling

Level 4 - medication management (access to medication history, warnings, and alerts)

Level 5 - connectivity to dispensing site

Level 6 - integration with an electronic medical record

Electronic Quality Data Submission (Performance and Accountability Measures):

Support the capture and reporting of quality, performance, and accountability measures to which providers/facilities/delivery.

Electronic Referral Management:

The ability to generate and/or receive summaries of relevant clinical information on a patient that are typically transferred between healthcare providers when a patient is referred to a specialist or admitted or discharged from a hospital.

Electronic Signature:

A digital signature, which serves as a unique identifier for an individual.

Emergency Medical Personnel:

Any persons that provide acute pre-hospital or out of hospital care.

Encryption:

The process of enciphering or encoding a message so as to render it unintelligible without a key to decrypt (unscramble) the message.

Error, Medical:

The failure of a planned action to be completed as intended or the use of a wrong plan to achieve an aim.

Error, Medication:

A medication error is any preventable event that may cause or lead to inappropriate medication use or patient harm while the medication is in the control of the health care professional, patient, or consumer. Such events may be related to professional practice, health care products, procedures, and systems, including prescribing; order communication; product labeling, packing and nomenclature; compounding; dispensing; distribution; administration; education; monitoring; and use.

Error, Systems (or Latent):

An error that is not the result of an individual's actions, but the predictable outcome of a series of actions and factors that comprise a diagnostic or treatment process.

Global Patient Index (GPI):

A common medical record number or algorithm that identifies patients across several institutions

Health Data (or Information) Exchange:

The process of transmitting health information between systems is often referred to as clinical messaging or health data exchange.

Health Information:

Information in any form (oral, written or otherwise) that relates to the past, present or future physical or mental health of an individual. That information could be created or received by a health care provider, a health plan, a public health authority, an employer, a life insurer, a school, a university or a health care clearinghouse. All health information is protected by state and federal confidentiality laws and by HIPAA privacy rules.

Health information technology:

Health informatics or medical informatics is the intersection of information science, medicine and health care. It deals with the resources, devices and methods required to optimize the acquisition, storage, retrieval and use of information in health and biomedicine. Health informatics tools include not only computers but also clinical guidelines, formal medical terminologies, and information and communication systems.

High Reliability Organizations:

Highly complex technologically intensive organizations that must operate as far as humanly possible to a failure free standard.

Health Level Seven (HL7):

An international community of healthcare subject matter experts and information scientists collaborating to create standards for the exchange, management and integration of electronic healthcare information. HL7 promotes the use of such standards within and among healthcare organizations to increase the effectiveness and efficiency of healthcare delivery for the benefit of all. It is the most widely used messaging standard and includes fields for: diagnostic results, notes, referrals, scheduling information, nursing notes, problems, and clinical trials data.

Health Insurance Portability and Accountability Act of 1996 (HIPAA):

The Health Insurance Portability and Accountability Act of 1996. HIPAA's Administrative Simplification provisions require the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data.

Home Health Agencies:

Home health agencies provide skilled care services in homes or alternative community settings. The Health Facilities and Emergency Medical Services Division is responsible for monitoring and evaluating the quality of health care services provided by certified home health providers, and enforces Medicare and Medicaid standards in home health agencies.

Hospice care:

Facility or program providing care for the terminally ill. Hospice care involves a team-oriented approach that addresses the medical, physical, social, emotional and spiritual needs of the patient. Hospice also provides support to the patient's family or caregiver as well. Hospice care is covered under Medicare Part A (Hospital Insurance).

Hospitals:

Any institution duly licensed, certified, and operated as a Hospital. "Hospital" does not include a convalescent facility, nursing home, or any institution or part thereof which is used principally as a convalescence facility, rest facility, nursing facility, or facility for the aged.

ICD-9 (International Classification of Disease, 9th Revision):

The 1972 revision of the international disease classification system developed by the World Health Organization.

ICD-9-CM (International Classification of Disease, 9th Revision, Clinical Modification):

The American modification of the ICD-9 classification system for both diagnoses and procedures.

ICD-10 (International Statistical Classification of Diseases and Related Health Problems, 10th Revision):

The 1992 revision of the international disease classification system developed by the World Health Organization.

ICD-10-CM (International Statistical Classification of Diseases and Related Health Problems, 10th Revision, Clinical Modification):

The American modification of the ICD-10 classification system, for field review release in 1998.

ICD-10-PCS (International Statistical Classification of Diseases and Related Health Problems, 10th Revision, Procedural Classification System):

A classification system for reporting clinical procedures, to accompany ICD-10-CM, developed in the US, for 1998 field review release.

Informatics:

The application of computer science and information science to the management and processing of data, information, and knowledge.

Interface:

Shared boundary between two functional units defined by various characteristics pertaining to the functions, physical interconnections, signal changes, and other characteristics as appropriate.

Interface to ADT System:

The interface between an HIE and the systems that are sources for admission, discharge and transfer (ADT) of patients in the care delivery setting and that are resident within care delivery institution.

Interface to ASP EHR System:

The interface between an HIE and Electronic Health Records (EHRs) that are maintained on ASP platforms (i.e. NexGen, AllScripts).

Interface to Claims System:

The interface between an HIE and the systems that are sources for or routing pathways for claims data that are resident within health plans and claims clearinghouses.

Interface to EKG System:

The interface between an HIE and the systems that are sources for EKG results that are resident within dispensing physician offices and hospitals.

Interface to Eligibility System:

The interface between an HIE and the source data of which people have eligibility for which type of benefits that are resident within health plans and are not infrequently web-enabled.

Interface to Formulary System:

The interface between an HIE and the systems that are sources for formulary status of specific drugs for specific health benefit designs and that are resident within pharmacy benefit management companies and hospitals.

Interface to Laboratory System:

The interface between an HIE and systems that are sources of laboratory data.

Interface to Pharmacy System:

The interface between an HIE and the systems that are sources for prescription data or that are resident within dispensing pharmacies, pharmacy benefit management companies and hospitals.

Interface to Practice Management System:

The interface between an HIE and the systems that are sources for the financial management systems of physician practices.

Interface to Provider List System:

The interface between an HIE and the systems that track the multiple providers and their identifying data that are resident within health plans, dispensing pharmacies, pharmacy benefit management companies laboratories, physician practices, and hospitals.

Interface to Provider Office EHR System:

The interface between an HIE and EHRs that are maintained in practice-specific systems (e.g. EPIC).

Interface to Radiology System:

The interface between an HIE and systems that are sources for radiological data.

Interface to Transcribed Reports System:

The interface between an HIE and the systems that are sources for transcribed reports. Typically these systems are based at a transcription service or at a hospital and contain admission and discharge notes and consultations, operative reports, and pathology and radiology results.

Interoperability:

When multiple information systems can seamlessly exchange health information messages, they are said to be interoperable. EMRs are said to be interoperable if they are able to exchange (transmit and receive) data using standardized data transmission (coding and messaging) formats (standards).

The International Organization for Standardization (ISO):

It is a worldwide federation of national standards bodies from some 130 countries, one from each country. ISO's work results in international agreements which are published as International Standards.

Keys:

A sequence of symbols that controls the operations of encryption and decryption.

Key Certificate:

A data record that authenticates the owner of a public key for an asymmetric algorithm. It is issued by a certification authority and is protected by a digital signature allowing the certificate to be verified widely. The certificate may also contain other fields beside the value to the key and the name of the owner, for example an expiration date.

Key stakeholders:

Is a person or organization that has a legitimate interest in a project or entity.

LOINC (Logical Observation Identifiers, Names, and Codes):

The LOINC databases provide sets of universal names and ID codes for identifying laboratory and clinical test results. The purpose is to facilitate the exchange and pooling of results, such as blood hemoglobin, serum potassium, or vital signs, for clinical care, outcomes management, and research.

Medication Matching:

The process of cross-linking the multiple possible medication identifiers naming conventions in a community from a variety of systems housing medication information and creating a master medication identifier with a key for cross-referencing the various community identifiers. For example there are hundreds of NDC codes for identical drugs as well as HCPCS codes that identify the same drug as NDC codes.

Medical Mistake:

A commission or an omission with potentially negative consequences for the patient that would have been judged wrong by skilled and knowledgeable peers at the time it occurred, independent of whether there were any negative consequences.

Medication Reconciliation (electronic):

Alerts providers in real-time to potential administration errors such as wrong patient, wrong drug, wrong dose, wrong route and wrong time in support of medication administration or pharmacy dispense/supply management and workflow.

Message Integrity:

Protecting a message against its unauthorized modification, often by the originator of the message generating a digital signature.

Messaging to Pharmacies:

The process of communicating electronically with pharmacies. This typically includes the cost of communication lines and processes between the HIE and pharmacies. This is necessary to support the e-prescribing function when that function includes the process of electronically sending a digital prescription to the pharmacy.

Messaging to Providers:

The process of communicating electronically with providers. This typically includes the cost of communication lines and processes between the HIE and provider terminals.

National Health Information Network:

The collective array of components that underlie nationwide interoperability, such as interconnection tools (mobile authentication, identification management, common web services architecture and security technologies); defined implementation regimens that are specified at the level of software code; common networking and communication tools to unify access and security; and mechanisms

for ensuring the sustainable operation of these components on a widespread and publicly available basis must be defined. On November 10, 2005, HHS Secretary Mike Leavitt announced the award of contracts totaling \$18.6 million to four groups of health care and health information technology organizations to develop prototypes for a Nationwide Health Information Network architecture.

Nebraska Telehealth Network:

the interactive videoconferencing that can be used in responding to an emergency and to allow citizens across the state to access health specialists without having to leave their home towns. The Nebraska Statewide Telehealth Network will directly connect 80 Nebraska hospitals, 20 local public health departments, Nebraska's state and regional public health labs, and key state agencies. The goal is to increase the quality, availability, and accessibility of healthcare throughout the state, particularly in rural areas of Nebraska, and to improve the readiness of the state to respond to terrorism-related or public health emergencies.

Near Miss:

An event or situation that could have resulted in an accident, injury or illness, but did not, either by chance or through timely intervention. Also known as close call or near hit.

Network:

A set of connected elements. For computers, any collection of computers connected together so that they are able to communicate, permitting the sharing of data or programs.

Network Connectivity:

The process used for maintaining connection for communication between the HIE and a data source (laboratory, radiology practice, physician practice, or hospital) and data user (physician practice or hospital).

Office of the National Coordinator for Health Information Technology (ONC, formerly referred to as ONCHIT):

The National Coordinator for Health Information Technology serves as the Secretary's principal advisor on the development, application, and use of health information technology; coordinates the Department of Health and Human Services' health information technology programs; ensures that health information technology policy and programs are coordinated with those of other relevant executive branch agencies; and to the extent permitted by law, develops, maintains, and directs the implementation of a strategic plan to guide the nationwide implementation of interoperable health information technology in both the public and private health care sectors that will reduce medical errors, improve quality, and produce greater value for health care expenditures, and coordinates outreach and consultation by the relevant executive branch agencies with the public and private sectors.

Order Entry:

The process of communicating health care provider orders through electronic, computerized processes.

OSI (Open Systems Interconnection):

An international standard for networking adopted by the ISO (International Organization for Standardization). This 7-layer model offers the widest range of capabilities for networking.

Outbreak Surveillance:

Support clinical health state monitoring of aggregate patient data for use in identifying health risks from the environment and/or population.

Patient permission:

Expressed consent or authorization from the patient

Patient Matching:

The process of cross-linking the multiple patient identifiers in a community from a variety of patient identifier sources and creating a master patient identifier with a key for cross-referencing the various community identifiers. This is also referred to as a record locator service.

Patient's Privacy:

For purposes of the HIPAA Privacy Rule, privacy means an individual's interest in limiting who has access to personal health care information. See also HIPAA Privacy Rule.

Patient Safety:

Freedom from accidental injury; ensuring patient safety involves the establishment of operational systems and processes that minimize the likelihood of errors and maximize the likelihood of intercepting them when they occur.

Personal health record (PHR):

Refers to computer-based patient records intended primarily for use by consumers, which may or may not interface with providers' electronic records. An electronic application through which individuals can maintain and manage their health information (and that of others for whom they are authorized) in a private, secure, and confidential environment.

Plan of care, progress or consultation notes:

Information maintained in the patient chart relating to management of health

Practice Acts:

A product, such as a statute, decree, or enactment, resulting from a decision by a legislative or judicial body

Privacy:

Right of an individual to control the circulation of information about him-/herself within social relationships; freedom from unreasonable interference in an individual's private life; an individual's right to protection of data regarding him/her against misuse or unjustified publication.

Private Key:

In asymmetric cryptography, the key which is held only by the user for signing and decrypting messages.

Public Health Outbreak Surveillance:

Supports clinical health state monitoring of aggregate patient data for use in identifying health risks from the environment and/or population.

Public Health Processor:

A software product that processes extracted data from health care provider systems for the purpose of tracking, trending, and reporting for public health reasons.

Public Key:

In asymmetric cryptography, the key which is published by the user to encrypt messages and so that others may verify his/her signature.

Public Key Certificate:

A data record that authenticates the owner of a public key for an asymmetrical key system. It is issued by a CA and is protected by a digital signature, allowing the certificate to be verified widely.

Public Key Infrastructure (PKI):

A conceptual framework that enables the encryption, decryption and electronic "signing" of data transmissions in a secure fashion within an open network environment.

Quality of care:

Quality is the degree to which health services for individuals and populations increase the likelihood of desired health outcomes and are consistent with current professional knowledge. Quality can be defined as a measure of the degree to which delivered health services meet established professional standards and judgments of value to consumers.

Radiologic information:

Information that applies to anything procedurally, surgically, or therapeutically that involves Radiology.

Regional Health Information Organization (RHIO):

A RHIO is an electronic network for exchanging patient health information among providers.

Rural Health Clinics:

A public or private hospital, clinic or physician practice designated by the federal government as in compliance with the Rural Health Clinics Act (Public Law 95-210). The practice must be located in a Medically Underserved area or a Health Professions Shortage Area and use a physician assistant and/or nurse practitioners to deliver services. A rural health clinic must be licensed by the state and provide preventive services. These providers are usually qualified for special compensations, reimbursements and exemptions.

Results Answer Matching:

The process of cross-linking the multiple possible answers to asking for a given result. For instance, asking for the results of a chest x-ray could yield a dictated report or a digital image of an x-ray. In any case, the case received must be matched across the type of result to a term identifying a common result.

Results Name Matching:

The process of cross-linking the multiple possible names of data results that can contain the same information. For instance a blood glucose reading can be called up by a blood glucose test, an SMA panel, or a glucometer result.

Results Review (Alerts to Providers):

The ability to interpret the clinical data that is entered about a patient using a set of rules or algorithms which will generate warnings or alerts at various levels of severity to a clinician. These are intended to make the clinician aware of potentially harmful events, such as drug interactions,

patient allergies, and abnormal results that may affect how a patient is treated, with the intention of speeding the clinical decision process while reducing medical errors. .

Risk:

The chance of a vulnerability being exploited

Risk Assessment:

An evaluation of the chance of vulnerabilities being exploited based on the effectiveness of existing or proposed safeguards or countermeasures.

Rules Engine:

A set of rules defined within a software process that converts clinical and administrative data streams into a meaningful representation of clinical quality markers to be used in functions such as pay for performance/quality data reporting.

Security:

In information systems, the degree to which data, databases, or other assets are protected from exposure to accidental or malicious disclosure, interruption, unauthorized access, modification, removal or destruction.

Security and privacy barriers:

A boundary or limit that presents maintenance of an individual's security and/or privacy

Sentinel Event:

An unexpected occurrence or variation involving death or serious physical or psychological injury, or the risk thereof. This is a proprietary term developed by The Joint Commission.

SNOMED International:

A nomenclature for use by all health services professionals developed in the US and updated at least semi-annually.

Statistical Deviation Detector:

Identifies variances from patient-specific and standard care plans, guidelines, and protocols.

Telehealth:

The use of telecommunications (i.e., wire, internet, radio, optical or electromagnetic channels transmitting text, x-ray, images, records, voice, data or video) to facilitate medical diagnosis, patient care, patient education and/or medical learning. Professional services given to a patient through an interactive telecommunications system by a practitioner at a distant site.

Third Party-General System:

Applications that are essential to the basic infrastructure of the system. They are the building blocks such as the technical platform the EHR system is built on such as, Windows, Linux, or MacIntosh, etc. Also what kind of database structure controls the system – SQL, Oracle, etc. When comparing license costs note if there are separate general system license costs or if these are rolled into the main cost. Also, will there be additional costs when the vendor upgrades their software and it is necessary to install a new version of the database or operating system. Make sure your infrastructure software will support any features you wish to add later on.

Training Services:

Consulting services offered by the vendor. They provide hands on training for all aspects of the system.

UMLS (Unified Medical Language System):

A long-term research project developed by the US National Library of Medicine to assist health professionals and researchers to retrieve and integrate clinical vocabularies from a wide variety of information sources. The goal is to link information from scientific literature, patient records, factual databases, knowledge-based expert systems, and directories of institutions and individuals in health and health services.

X12:

A committee chartered by the American National Standards Institute (ANSI) to develop uniform standards for inter-industry electronic interchange of business transactions—electronic data interchange (EDI).

Appendix E

Taxonomy for Consumers

The language used in the health information technology literature and conversations is often technically specific and unique. The following taxonomy and definitions is provided as a basic resource to assist consumers in achieving an understanding of computer technology and how it relates to sharing of health information.

Access:

The process of putting data into or taking data from a computer system or storage device.

Active conditions/diagnoses:

The list of medical problems that a doctor or health care provider has indicated a patient has.

Active medications:

Medications a patient is actively taking.

AHRQ:

An abbreviation used for the Agency for Healthcare Research Quality, a part of the U.S. Department of Health and Human Services.

Ambulatory surgical centers:

Ambulatory surgery centers (ASCs) provide elective same-day or outpatient surgery. They do not offer emergency care.

American National Standards Institute (ANSI):

ANSI is a broad based agency charged with overseeing voluntary standards development for everything from computers to household products.

American Society for Testing and Materials (ASTM):

ASTM develops standards on characteristics and performance of materials, products, systems, and services. This group is developing standards on the Continuity of Care Record.

Application Service Provider (ASP):

A company that creates information technology solutions for computer software and hardware to communicate and exchange information.

Architecture:

This is the map or description of how information technology is assembled and connected together.

Audit trail:

A record of any computer system activity which lets computer professionals see what has happened to computer data.

Authentication:

A method to be sure that a person who accesses information from electronic health information products (such as a health record or health information exchange system) is actually that person.

Authorization:

The set of permissions on a computer that let a person access health information.

Biometric Authentication Technology:

Technology that uses fingerprint, voice pattern, retina scan, or signature dynamics, to uniquely identify a person.

Chart Review:

A review of a patient's medical record some time after they have received care and the information is written or put into their record. This is usually done to learn information needed to improve the processes of providing health care.

Clinical Data Repository:

A computer that stores the health information for many patients in a way that makes it possible for many persons who have been given permission to access it.

Clinical Messaging:

Communicating a patient's health information between their health care providers or between the patient and health care provider using computers.

Clinical records (medical records):

A written record of the patient's medical care provided. It is organized by date and includes the information that comes from the patients care providers and facilities such as laboratories.

Computerized Provider Order Entry (CPOE):

A computer system that can be used by a patient's health care provider (doctor, nurse, pharmacist, therapist, etc.) to order medicines and treatments for that patient. It replaces the use of paper.

Confidentiality:

When the patient has given permission to someone else to have their personal health information, this is that person's (or organizations) obligation to protect the personal information so others can not have access to it.

Continuity of Care Record:

A core dataset to be sent to the next healthcare provider whenever a patient is referred, transferred, or otherwise uses different clinics, hospitals, or other providers.

Data Center:

The physical space and hardware used by computers that exchange patient health information to house its operations.

Data Integrity:

The accuracy and completeness of data, to be maintained by appropriate security measures and controls. Preservation of the original quality and accuracy of data, in written or in electronic form.

Data Recovery Services:

A method to safely store duplicate data and recreate the data should the loss of health information data from the computer occur.

Data Security:

The processes used to make sure that your health information that is stored on a computer is protected from others getting access to it who do not have permission. It also protects your information from being destroyed or changed.

Decryption:

The technique of using mathematical procedures to "unscramble" data so that a message that cannot be interpreted (encrypted) can now be interpreted.

Digital Signature:

An electronic way to make the signature of each person who signs onto any aspect of a computer system be considered genuine for that person.

Doctor Matching:

This is a computer method of assuring that the doctor's identity on different health care systems can be matched so that the use of records from multiple systems for a doctor is the correct set of records for that doctor.

e-Laboratory:

The electronic delivery of laboratory results to health care providers offices so that such data may be viewed and used by the health care provider.

Electronic Billing Support:

The ability to contact the payer before the patient is seen and get a response that indicates whether or not the services to be rendered will be covered by the payer.

Electronic Health Record (EHR):

See electronic medical record.

Electronic Imaging Results Delivery:

The ability to get an x-ray for a patient by sending it from a computer in one location to another.

Electronic Medical Record (EMR):

An electronic form of your medical record that is used at the time care is provided to you by a health professional.

Electronic Referral Management:

The ability to generate and/or receive summaries of relevant clinical information on a patient that are typically transferred between healthcare providers when a patient is referred to a specialist or admitted or discharged from a hospital.

Electronic Signature:

A digital signature, which serves as a unique identifier for an individual.

Emergency Medical Personnel:

Any persons that provide acute pre-hospital or out of hospital care that is needed during an emergency.

Encryption:

The process of coding a computer message so someone else cannot read it without a computer method to unscramble the message.

Electronic Prescribing (e-prescribing):

A prescription for medication is written on a computer. It may be printed on a computer printer and given to the patient to take to a pharmacy. It may also be sent through the internet to a pharmacy and the patient picks up the medication without ever having to carry the prescription to the pharmacy.

Error, Medical:

The wrong thing is done in the care of a patient or the wrong plan is followed when providing care. It is not intentional.

Error, Medication:

The wrong medication, dose, or method of taking the medication is prescribed by the doctor, dispensed by the pharmacist, or consumed by the patient. It also includes mistakes made when counseling a patient or determining how the patient is responding to their treatment.

Error, Systems (or Latent):

An error that is not the result of an individual's actions, but the result of a series of actions in a diagnostic or treatment process.

Global Patient Index (GPI):

a common medical record number used to identify the patient's record when it is being electronically sent or used by more than one office or health care facility.

Health Care Interoperability:

Assures the clear and reliable communication of meaning of health information.

Health Data (or Information) Exchange:

The process of transmitting health information between two different places (example a doctors office and hospital) by using computers.

Health Information:

Information in any form (oral, written or otherwise) that relates to the past, present or future physical or mental health of a person. That information could be created or received by anyone who has any role in providing care to a person, including the person directly. All health information is protected by state and federal confidentiality laws and by HIPAA privacy rules.

Health Information Technology:

Health information technology is the use of computers and related devices to assist in improving care through access to information.

High Reliability Organizations:

Highly complex technologically intensive organizations that must operate as far as humanly possible to a failure free standard.

Health Insurance Portability and Accountability Act of 1996 (HIPAA):

The Health Insurance Portability and Accountability Act of 1996. The Department of Health and Human Services is required to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. This act provides guidance about the security and privacy of health data for patients.

Home Health Agencies:

Home health agencies provide skilled care services in homes or alternative community settings.

Hospice Care:

Facility or program providing care for the terminally ill.

Hospitals:

Any institution duly licensed, certified, and operated as a Hospital.

ICD-10-CM (International Statistical Classification of Diseases and Related Health Problems, 10th Revision, Clinical Modification):

These are the official names of the medical conditions that are placed in the patients medical chart once a diagnosis is made.

ICD-10-PCS (International Statistical Classification of Diseases and Related Health Problems, 10th Revision, Procedural Classification System):

A classification system for reporting clinical procedures, to accompany ICD-10-CM.

Medication Matching:

The process of identifying medications correctly when there are multiple ways in electronic data systems (pharmacy computers, medical office computers, and so on) of identifying the same medication.

National Health Information Network:

A nationwide network of computer services and providers that can exchange health information on behalf of providing health care for a patient. This is in development.

Nebraska Telehealth Network:

A form of interactive videoconferencing that can be used in responding to an emergency and to allow citizens across the state to access health specialists without having to leave their home towns.

Network:

Any collection of computers connected together so that they are able to communicate, permitting the sharing of data or programs.

Office of the National Coordinator for Health Information Technology:

The National Coordinator for Health Information Technology is appointed by the Secretary of Health and Human Services to lead health information technology development and use for the United States.

Outbreak Surveillance:

Monitoring of aggregate patient data to identify health risks from the environment and/or population.

Patient Matching:

The process of cross-linking the multiple patient identifiers in a community from a variety of patient identifier sources and creating a master patient identifier with a key for cross-referencing the various community identifiers. This is also referred to as a record locator service.

Patient Permission:

When the patient gives consent or provides authorization for something to occur related to their health care or information.

Patient's Privacy:

Privacy is the term used that allows the patient to limit who has access to personal health care information. See also HIPAA Privacy Rule.

Patient Safety:

Freedom from accidental injury; ensuring patient safety involves the establishment of operational systems and processes that minimize the likelihood of errors and maximize the likelihood of intercepting them when they occur.

Personal Health Record (PHR):

Refers to computer-based patient records intended primarily for use by consumers, which may or may not interface with providers' electronic records.

Plan of care, progress or consultation notes:

Information maintained in the patient chart relating to management of health

Privacy:

Right of an individual to control the circulation of information about him-/herself. This includes health information. Freedom from unreasonable interference in an individual's private life; an individual's right to protection of data regarding him/her against misuse or unjustified publication.

Public Health Outbreak Surveillance:

Supports clinical health state monitoring of aggregate patient data for use in identifying health risks from the environment and/or population.

Public Health Processor:

A computer software product that takes data from patient's health care record stored data for the purpose of tracking, trending, and reporting for public health reasons.

Quality of Care:

The degree to which delivered health services meet established professional standards and judgments of value to consumers.

Regional Health Information Organization (RHIO):

A RHIO is an electronic network for exchanging patient health information among providers.

Risk:

The chance of a vulnerability being exploited. The chance that a person's private information will be used purposefully in a way by someone else that ultimately incurs some harm.

Risk Assessment:

An evaluation of risk (see definition) based on the effectiveness of existing or proposed safeguards or countermeasures.

Rural Health Clinics:

A public or private hospital, clinic or physician practice designated by the federal government as in compliance with the legal requirements of the Rural Health Clinics Act (Public Law 95-210).

Security:

In information systems, the degree of data protection.

Security and privacy barriers:

A boundary or limit that prevents or challenges a person's security or privacy.

Sentinel Event:

A major negative event, such as serious injury or death that occurs in the course of delivering healthcare.

Telehealth:

The use of telecommunications by a health care professional (i.e., wire, internet, radio, optical or electromagnetic channels transmitting text, x-ray, images, records, voice, data or video) to provide care to a person when face-to-face care is not realistic or possible.