



Review & Recommendations

A healthier Iowa through the use and exchange of electronic health information

Iowa e-Health Project



Privacy and Security Report

December 2009

Improve patient centered health care and population health

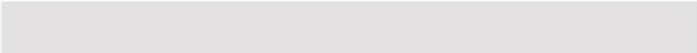
Secure Patient Data



Protect patient privacy



Electronic Health Information Executive Committee and Advisory Council
Iowa Department of Public Health



Executive Summary:

This report is written in response to House File 811, 83rd General Assembly, Section 135 that requires the e-Health Executive Committee to review the electronic exchange of patient information by health care providers. The use and exchange of electronic health information affords the opportunity to improve patient centered health care and population health. A statewide health information exchange (HIE) will provide a public good that will improve the quality of health care, assure patient safety, increase efficiency in health care delivery, and promote and protect the health of Iowans.

Current Iowa laws¹ and policies hinder the exchange of health information to provide the best care to patients. Ambiguity and different interpretations of the laws and policies result in practices that are more restrictive than federal standards, primarily defined through HIPAA². Furthermore, traditional patient privacy laws assumed paper medical records were to be used in provider practices and information would be shared among providers using photocopies or faxes of patient information. As providers transition to electronic health records (EHR), and as information becomes available electronically through a statewide HIE, laws and policies will need to be modified to reflect the modernized workflow.

This report serves as an introduction to the privacy and security framework being developed by the Iowa e-Health Project. The report provides an analysis of barriers to health information exchange (e.g., state laws, consent, liability, and data sharing agreements) and includes preliminary recommendations to overcome the identified barriers. The foundation for the report comes from Health Information Security and Privacy Collaboration (HISPC), a national project sponsored by Office of the National Coordinator for Health Information Technology (ONC) and Agency for Healthcare Research and Quality (AHRQ).

| Barriers | | Recommendations |
|----------|---|---|
| 1. | State restrictions on sharing information from specialty records (i.e., HIV/AIDS, substance abuse, mental health, genetics, etc.) among providers | Consider statutory changes in Iowa law to allow protected health information to be exchanged among providers for treatment-related purposes without additional patient consent * |
| 2. | Unclear patient consent policies for HIE | Establish clear patient consent policies within the HIE privacy and security framework * |
| 3. | Concern about provider liability when participating in an HIE | Develop an appropriate safe harbor policy within the HIE privacy and security framework * |
| 4. | Different interpretations among providers about HIPAA legal requirements and HITECH Act ³ implications on HIPAA | Prepare and disseminate a legal interpretation for providers of HIPAA requirements and recent HITECH Act implications on HIPAA |
| 5. | Inconsistent patient identifiers across provider networks | Establish a master patient index and record locator service to locate and match patient information across provider networks * |
| 6. | Consumer and provider awareness of the value and need for health IT | a) Provide resources to execute a comprehensive communication strategy to educate and build awareness among consumers and providers b) Establish a consumer advisory council to work in conjunction with the e-Health Executive Committee and Advisory Council * |

** The e-Health Executive Committee is currently working on these recommendations. The e-Health Executive Committee anticipates preparing a comprehensive e-Health legislative package with assistance from the Iowa Attorney General's Office for consideration during the 2011 Iowa legislative session.*

¹ Iowa Code Section 141A (HIV/AIDS) and Iowa Code Chapters 228 and 229 (Mental Health)

² Health Insurance Portability and Accountability Act of 1996. Pub. L. No. 104-191, 110 Stat. 1936 (1996).

³ American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, (February 17, 2009). Division A Title XIII: Health Information Technology for Economic and Clinical Health Act (HITECH).

Background on Privacy and Security and the Exchange of Health Information:

Health care data systems are much different than typical transactional data systems. Data are more personal and complex, collected from many different providers throughout a person's lifetime. While maintaining patient privacy protections, health care data must also be shared with other providers to provide the best possible care to the patient. It is imperative that security controls in health care data systems do not negatively impact or slow down this delivery of care to a patient, especially in emergency situations.

With the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act in February 2009, as part of the American Recovery and Reinvestment Act (ARRA)⁴, the federal government has made health information technology (health IT) a national priority. Two significant components of health IT are electronic health records (EHR) and health information exchange (HIE). EHRs are used to collect and store patient health information and an HIE facilitates sharing of essential patient information from EHRs across the boundaries of individual provider settings. Together, EHRs and a statewide HIE will allow health care providers access to real-time health information. Real-time health information helps *providers* make the best health care decisions and provides *consumers* with continuity of care regardless of the provider they visit. A key premise, according to Dr. David Blumenthal, National Coordinator for Health Information Technology, is "information should follow the patient, and artificial obstacles – technical, business related, bureaucratic – should not get in the way."⁵

Opportunity to be More Secure: There are some potential risks associated with electronic health information (e.g., data entry errors, data and identity theft). However, there are similar risks with paper record processes. Current EHR and HIE technology has the opportunity to provide greater privacy and security protections than previously possible with traditional record systems. Unlike paper health records, certified EHRs are password protected and encoded to ensure only authorized personnel have access to patient information. An audit log automatically records when and by whom an EHR is viewed, modified, or shared. Data backups regularly archive patient data, and in the event of a disaster (e.g., flood, fire, tornado), files can be easily restored to the original location, or an alternate care setting.

Importance of Policymaking: For a statewide HIE to be successful, patients must trust their health information is kept confidential and secure, and providers must be able to access their patients' information to make the best health care decisions. Privacy policies and HIE security controls can provide assurances to consumers; however it is important to find the right balance in policymaking to allow providers access to the information they need to help their patients. Strict privacy policies can slow the adoption of the statewide HIE and decrease the value of the exchange for providers. Policies that are too lenient can negatively impact the integrity of the statewide HIE and reduce trust and perceived value of the exchange of health information.

The following abstracts highlight the importance of policymaking to support health IT:

- National Governor's Association, "Preparing to Implement HITECH: A State Guide for Electronic Health Information Exchange" (August 2009). *Abstracted quote: States should revise state policies and laws and help providers adopt statewide standards on privacy policy and practices.*

⁴ American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, (February 17, 2009). Division A Title XIII: Health Information Technology for Economic and Clinical Health Act (HITECH).

⁵ Dr. David Blumenthal, email to Health IT News e-mail list, November 12, 2009, http://healthit.hhs.gov/portal/server.pt?open=512&objID=1406&parentname=CommunityPage&parentid=23&mode=2&in_hi_userid=11113&cached=true.

- NET Institute Working Paper No. 07-16, “Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records” (February 2009). www.informs.org/site/ManSci/. *Abstracted quote: State privacy laws that restrict a hospital's release of health information reduce the likelihood that facilities will adopt electronic medical records by more than 24%.*
- SCMagazineUS, “Labor Pains: An Increasing number of patient medical records go digital, health care security pros face some trying times” (October2009). *Abstracted quote: We have on one hand the need to protect the privacy and security of our patients' records. But on the other hand, we have to be able to completely expose the records and provide timely access to the records for treatment and medical care. And so we have to be able to do both in a way that preserves the security and the integrity of the data but also does not create impediments for physicians.*
- Nevada statute: [NRS 439.538 passed in 2007]. *Abstract: If a covered entity transmits electronically individually identifiable health information in compliance with the provisions of the HIPAA, the covered entity is, for purposes of the electronic transmission, exempt from any state law that contains more stringent requirements or provisions concerning the privacy or confidentiality of individually identifiable health information.*
- Nebraska statute: [Neb. Rev. Stat. § 44-919.] *Abstract: Licensees that comply with HIPAA are not subject to the patient authorization provisions of Nebraska sections 44-916 to 44-920.*

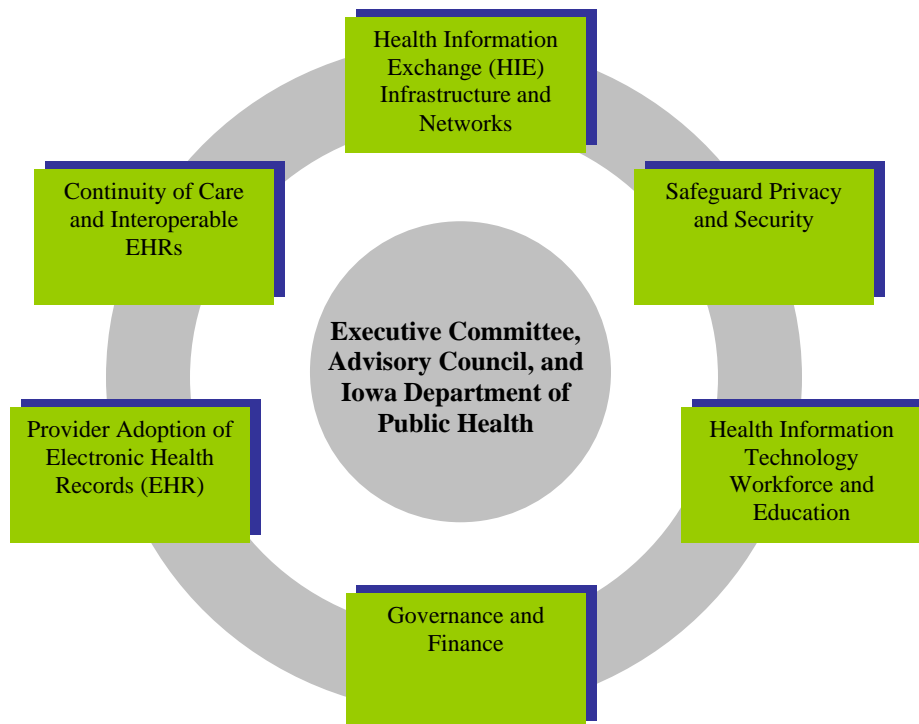
Security and Interoperability: Many health IT vendors have experience developing security processes and standards that are appropriate within a single provider network. However, security processes and standards among disparate provider data systems are different and require different health IT vendor competencies. Interoperability standards, such as Health Level 7 (HL7), are being developed, but the health IT industry is still perceived to be behind in security standards and architecture⁶. With undersized IT security budgets and limited funding available to support extensive health IT goals, it is important for the health IT vendor community to take initiative to develop more advanced and broad interoperability strategies and security infrastructure.

⁶ Armstrong, I. (2009, October) Labor Pains: As an increasing number of patient medical records go digital, health care security pros face some trying times. *SC Magazine*. 32-37.

Health IT Planning in Iowa:

The collaborative effort to plan and promote health IT in Iowa has come to be known as the Iowa e-Health Project. In January 2009, Iowa Department of Public Health (IDPH) convened the first Electronic Health Information (e-Health) Executive Committee and Advisory Council [2008 Iowa Acts, Chapter 1188 (HF 2539)]. Several multi-stakeholder workgroups were also established to provide subject matter expertise for components of the Iowa e-Health Project planning process. The executive committee, advisory council, and workgroups are comprised of diverse stakeholders from public and private entities including providers, professional associations, government, payers, educators, researchers, and consumers.

Figure 1: Iowa e-Health Project Workgroups and Advisory Bodies



One of the workgroups, Safeguard Privacy and Security, was formed to make recommendations for policies and procedures that will provide protections to consumers and providers involved or impacted by the exchange of electronic health information. The workgroup identified the following goal and objectives:

Goal 4: Safeguard privacy and security of electronic health information

Objectives:

- 4.1 Develop a privacy and security framework
- 4.2 Establish privacy and security policies and procedures for pilot HIE implementations
- 4.3 Assess potential risks and liabilities to providers and consumers
- 4.4 Formulate data sharing strategies and data use agreements

This goal is reflected in the Iowa Health Information Technology Plan⁷, which was approved by the e-health Executive Committee in June 2009 and the State Board of Health in July 2009 and delivered to the Iowa Legislature in July 2009 as requested 2008 Iowa Acts, Chapter 1188 (HF 2539).

Several of the current Safeguard Privacy and Security workgroup members were involved in Health Information Security and Privacy Collaboration (HISPC), a multi-state project sponsored by Office of the National Coordinator for Health IT (ONC) and Agency for Healthcare Research and Quality (AHRQ). HISPC intended to address the privacy and security challenges presented by electronic health information exchange (HIE). Iowa's HISPC effort was led by the Iowa Foundation for Medical Care and a multi-stakeholder steering committee, the project resulted in multiple deliverables including: 1) assessment of privacy and security barriers; 2) results from urban and rural consumer focus groups; 3) proposed privacy and security solutions; 4) patient consent framework for treatment scenarios; 5) continuity of care document exchange pilot; 6) legal and legislative recommendations; and 7) model interorganizational data-sharing agreements⁸. Participation in HISPC has provided an opportunity for Iowa to review and understand state-specific privacy and security challenges and provides the foundation for workgroup discussions and development of this report.

The Iowa e-Health Project plans to engage the Iowa Attorney General's Office in the development of a robust privacy and security framework for the statewide HIE. This framework will be based on nationally recognized privacy and security standards (e.g., HIPAA) and build on previous privacy and security studies (e.g., HISPC). The framework will establish privacy policies and practices and support harmonization of intra and interstate data exchange laws and agreements. HIE security controls (e.g., role-based security and audit trails) will also be developed through a contract with a technology vendor (to be identified) to support the policies and practices identified in the privacy and security framework. Role-based security will provide identification, authentication, and access controls to ensure patient records are only viewed by authorized provider sites and registered users. Security audit trails will be used to ensure accountability by monitoring all activity by all users within the HIE. Reports or alerts generated from audit records will provide transparency in how records have been used and will allow Iowa to monitor compliance and appropriateness of HIE activities.

⁷ Iowa e-Health Project, "Iowa Health Information Technology Plan" (July 2009).
www.idph.state.ia.us/hcr_committees/electronic_health_info.asp

⁸ Health Information Security and Privacy Collaboration (HISPC). "Resource Guide for the State of Iowa" (December 2007).

Review and Recommendations:

Assessing barriers to electronic health information exchange and formulating privacy and security strategies and protections is important to help secure trust and support for a statewide HIE. Leveraging previous work conducted through HISPC and lessons learned in Iowa and other states, the Iowa e-Health Project has identified the following barriers to exchange of health information among health care providers.

1. STATE RESTRICTIONS ON SHARING INFORMATION FROM SPECIALTY RECORDS (I.E., HIV/AIDS, SUBSTANCE ABUSE, MENTAL HEALTH, GENETICS, ETC.) AMONG PROVIDERS

HIPAA, other federal laws, and state law recognize HIV/AIDS, substance abuse, mental health, genetics information, etc. to be sensitive types of health information that warrant heightened scrutiny and privacy and security protections. State and federal laws have been developed to address patient concern that information regarding these types of treatment will: 1) be accessed by health plans and employers, for example, to deny insurance coverage or job promotions; 2) be “hacked into” and shared inappropriately, causing social ostracizing or personal embarrassment; 3) be “tracked” or “watched” by the government; or 4) in general, fall into the wrong hands and violate personal privacy.

In Iowa, state law⁹ provides heightened security above HIPAA regulations to protect sensitive patient information. These regulations limit the exchange of important patient information for treatment related purposes. The inability to share such information, even among a patient’s regular care providers, can impact treatment decisions and compromise patient safety (e.g., providers may not have record of medications prescribed to the patient).

Recommendation #1: Consider statutory changes in Iowa law to allow protected health information to be exchanged among providers for treatment-related purposes without additional patient consent

Exchanging health information, including but not limited to protected health information, facilitates continuity and improved quality of health care for patients. Statutory language allowing the exchange of health information for treatment-related purposes benefits the patient while maintaining the purpose and integrity of all privacy and security laws. This language could be part of the comprehensive e-Health legislative package the e-Health Executive Committee anticipates preparing for consideration for the 2011 Iowa legislative session.

2. UNCLEAR PATIENT CONSENT POLICIES FOR HIE

There are various approaches in determining when clinical data can be included in the statewide HIE. Some HIEs include only those patients that have “opted-in” to the HIE by signing an enrollment form. The vast majority of operational HIEs nationwide include all patients in the HIE unless they have “opted-out” of the HIE by signing a waiver form. Beyond the foundational opt-in or opt-out policy, there are also various levels to which the policy can be applied (i.e., can patients opt to have certain types of records excluded).

Recommendation #2: Establish clear patient consent policies within the HIE privacy and security framework (*under development through the Iowa e-Health Project*)

Patient consent policies, as well as the mechanism for implementation, will be clearly delineated and communicated as part of the HIE privacy and security framework. The Iowa e-Health Project will build this framework to allow incremental development of HIE policies over time, enable appropriate, inter-

⁹ Iowa Code Section 141A (HIV/AIDS) and Iowa Code Chapters 228 and 229 (Mental Health)

organizational health information exchange, and meet other important state policy requirements such as those related to public health and vulnerable populations.

3. CONCERN ABOUT PROVIDER LIABILITY WHEN PARTICIPATING IN AN HIE

Some health care providers are apprehensive about releasing electronic health information due to liability risks. Providers fear that if they participate in the HIE and someone else exposes their patient records, they will be held liable. A conservative approach by providers with this apprehension is to make the decision to not share any records, which could limit the amount of information available in the statewide HIE, thereby limiting the benefits and value of the HIE.

Recommendation #3: Develop an appropriate safe harbor policy for providers within the HIE privacy and security framework (*under development through the Iowa e-Health Project*)

The Iowa e-Health Project will assess the need, precedence, and feasibility of a safe harbor policy to include within the HIE privacy and security framework. Safe harbors can be used to reduce provider liability when exchanging records through the HIE on the condition that actions were performed according to standards (e.g., use of encryption) and in good faith (e.g., for treatment purposes).

4. DIFFERENT INTERPRETATIONS AMONG PROVIDERS ABOUT HIPAA LEGAL REQUIREMENTS AND HITECH ACT IMPLICATIONS ON HIPAA

The use of different terminology between HIPAA requirements and Iowa law can create confusion and an additional layer of legal scrutiny when determining whether health information can be legally exchanged under certain circumstances. Additionally, some providers may not be aware of expanded HIPAA provisions in the recent HITECH Act. In these cases, providers may interpret regulations differently, which may result in nonstandard practices that make intra and interstate health information exchange difficult.

Recommendation #4: Prepare and disseminate a legal interpretation for providers of HIPAA requirements and recent HITECH Act implications on HIPAA.

Within the HIE privacy and security framework (see recommendations #2 and #3), or as a separate report, it would be helpful to have a legal interpretation of HIPAA requirements and a clear analysis of HITECH Act implications on providers. This would help promote consistency in interpretation across provider organizations. The Iowa Attorney General's Office, or other legal consulting organization on behalf of the Iowa Attorney General's Office or the Iowa e-Health Project, is the ideal source for the interpretation and dissemination.

5. INCONSISTENT PATIENT IDENTIFIERS ACROSS PROVIDER NETWORKS

To successfully exchange health information among providers, there must be a mechanism to correctly match patients with their clinical data. Most often the identifier is a patient number assigned by each provider office. With the heightened concern of identity theft, the use of the social security number as an identifier is becoming less desirable. Additionally, patient numbers assigned by each provider office make it difficult to confirm a patient's identity and link patient information across disparate provider systems.

Recommendation #5: Establish a master patient index and record locator service to locate and match patient information across provider networks. (*under development through the Iowa e-Health Project*)

The Iowa e-Health Project is developing requirements for a master patient index (MPI) and record locator service (RLS) to locate and match patient information across provider networks through the statewide

HIE. In the absence of a single, standardized patient identifier (e.g., social security number, national patient identification number), technology and algorithms used with an MPI and an RLS can link patient data from disparate provider networks and create data exchange opportunities. This approach is different than establishing a single patient identifier. While the single patient identifier could simplify the record matching process, there are privacy and security implications to be studied. If a decision was made to issue a single patient identifier, this decision would likely come from the federal government in the form of a national patient identifier, rather than a number uniquely issued by each state.

6. CONSUMER AND PROVIDER AWARENESS OF THE VALUE AND NEED FOR HEALTH IT

With aggressive timelines for health IT adoption nationally, neglecting comprehensive consumer and provider education can result in fear and setbacks. Consumers and providers need to understand the benefits and potential impact of a statewide HIE and must have an opportunity to obtain accurate information and voice their concerns. Based on previous assessments and focus groups, concerns include, but are not limit to: 1) who has access to my (or my patient's) information; 2) how do I know if the data contained in my (or my patient's) record is accurate; and 3) is there potential for my (or my patient's) identity to be stolen.

Recommendation #6a: Provide resources to execute a comprehensive communication strategy to educate and build awareness among consumers and providers

As part of the state HIE grants available through the HITECH Act, the Iowa e-Health Project will develop a communication plan that outlines key messages to: 1) help consumers and providers understand the meaningful uses and value of health IT (e.g., patient safety, improved quality, and continuity of care); 2) instill consumer and provider confidence in a statewide HIE (e.g., privacy and security controls); and 3) provide support to provider groups in educating their patients. The communication plan will propose diverse communication methods and forums appropriate for different types of audiences (e.g., providers and consumers) and locations (e.g. rural and urban). The communication plan will also establish mechanisms for the Iowa e-Health Project to receive feedback, questions, and concerns from providers and consumers. Funding has been secured to develop the plan, however additional funding resources will need to be identified to execute the communication strategy to raise broad awareness and support for a statewide HIE in Iowa.

Recommendation #6b: Establish a consumer advisory council to work in conjunction with the e-Health Executive Committee and Advisory Council (under development through the Iowa e-Health Project)

To ensure broad approval and support for health IT, including but not limited to a comprehensive privacy and security framework, the Iowa e-Health Project needs to engage consumers and vocal consumer organizations in health IT planning and implementation. Iowa has learned from other HIE initiatives that the most vocal consumers are likely to become the strongest advocates for the system if provided the opportunity to voice concerns and be involved in policy decisions throughout planning and implementation. Since planning is well underway in Iowa, it is imperative to expand consumer involvement as quickly as possible. There are currently two consumer members of the e-Health Executive Committee and Advisory Council, but an additional forum for consumers to discuss health IT priorities, concerns, and expectations would strengthen consumer awareness and help maintain a consumer focus for health IT activities. A consumer advisory council is an approach recommended by previous HIE studies (e.g., HIM Principles in Health Information Exchange¹⁰) and seen in several other states (e.g., New York¹¹, North Carolina¹², Arizona¹³).

¹⁰ American Health Information Management Association. "HIM Principles in Health Information Exchange: RHIO Checklist" (2007).

¹¹ New York eHealth Collaborative. nyhealth.org/consumer-advocacy. Accessed October 2009.

¹² North Carolina Consumer Advisory Council on Health Information. www.nchica.org/GetInvolved/CACHI/intro.htm. Accessed October 2009.

Conclusion:

To facilitate the electronic exchange of health information while maintaining appropriate levels of consumer privacy, Iowa, like many other states, needs to establish a comprehensive HIE privacy and security framework. This framework will support the broader Iowa e-Health Project and its vision for a healthier Iowa through the use and exchange of electronic health information.

Iowa Department of Public Health and the e-Health Executive Committee and Advisory Council are engaged in planning activities to develop a statewide HIE. This includes but is not limited to a privacy and security framework and a comprehensive legislative package that may be needed to implement HIE policies. As planning and implementation activities continue, content of this report will continue to evolve. For current information about the Iowa e-Health Project, visit www.idph.state.ia.us/hcr_committees/electronic_health_info.asp.

With complementary policies and a privacy and security framework to support a statewide HIE, Iowa will leverage the potential for health IT to improve patient centered health care and population health and elevate the quality, safety, and efficiency of health care available to Iowans.

¹³ Arizona Health-e Connection. www.azhec.org/committees.jsp. Accessed October 2009.

Definitions:

| | |
|-------------------------|---|
| ARRA | <i>American Recovery and Reinvestment Act:</i> Also commonly referred to as the “stimulus bill” or “stimulus package,” the ARRA was signed into law February 17, 2009 and provides \$787 billion to promote economic recovery. |
| CCHIT | <i>Certification Commission for Health Information Technology:</i> CCHIT established criteria for functionality, security, and interoperability of health IT systems. CCHIT certifies EHRs and through a public-private process. |
| EHR or EMR | <i>Electronic health record or electronic medical record:</i> EHRs and EMRs are used to collect and store relevant patient health information electronically. EHRs may include computerized physician order entry, electronic prescribing, and decision-support functionality to improve patient safety and quality of care. |
| HIT or Health IT | <i>Health information technology:</i> Health IT, also shortened to “HIT,” refers to a range of electronic or computerized tools, such as EHRs and the HIE that enable providers to access and share electronic health information. |
| HIE | <i>Health information exchange:</i> The HIE is the infrastructure that facilitates and supports the exchange of electronic health information among clinical and population health settings. |
| HIPAA | <i>Health Insurance Portability and Accountability Act:</i> Issued by the U.S. Department of Health and Human Services in 1996, HIPAA establishes standards for the use and disclosure of health information and consumer privacy rights to understand and control how their information is used. A goal of HIPAA is to assure health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care. |
| HISPC | <i>Health Information Security and Privacy Collaboration:</i> HISPC is a multi-state, collaborative project funded by the Agency for Healthcare Research and Quality. HISPC has worked to address the privacy and security challenges presented by electronic health information exchange across the country. |
| HITECH | <i>Health Information Technology for Economic and Clinical Health Act:</i> A division within ARRA stimulus bill, the HITECH Act includes \$19.2 billion in funding provisions for health IT. |
| ONC or ONC-HIT | <i>Office of the National Coordinator Health Information Technology:</i> ONC-HIT, also shortened to ONC, is a program within the Office of the Secretary for the U.S. Department of Health and Human Services. ONC-HIT is the federal entity responsible for coordination of nationwide efforts for implementation and use of electronic health information exchange. |
| Treatment | <i>Treatment:</i> The provision, coordination, or management of health care and related services by one or more providers, including the coordination or management of health care by a provider with a third party; consultation between providers relating to a patient; or the referral of a patient for health care from one provider to another . |