

**REPORT FROM THE HEALTH INFORMATION
PROTECTION TASKFORCE TO THE STATE
ALLIANCE FOR E-HEALTH**

AUGUST 15, 2007

This report was financed by funds provided by the US Department of Health and Human Services, Office of the National Coordinator for Health IT (ONCHIT) under a contract with the National Governors Association for the State Alliance for e-Health. The report contents do not necessarily represent the official views of ONCHIT.

LETTER FROM CO-CHAIRS OF THE HEALTH INFORMATION PROTECTION TASKFORCE

Dear Members of the State Alliance,

The members of the Health Information Protection Taskforce are pleased to submit this report to the State Alliance for e-Health. The report reflects accomplishments of the Health Information Protection Taskforce to date, and advances recommendations it believes are necessary to help states address challenges to protecting the privacy and security of health information in an electronic exchange environment.

The Health Information Protection Taskforce worked under the charge provided by the State Alliance for e-Health when identifying findings, policy statements, and recommendations outlined in this report. The Taskforce's report outlines findings and recommendations with respect to the current status of state privacy laws, security challenges to electronic health information exchange, implementation of federal privacy requirements, and consumer education.

The Taskforce sought the expertise and perspectives of stakeholders to guide its deliberations and in crafting the recommendations. The Taskforce also worked in coordination with the states participating the Health Information Security and Privacy Collaboration—33 states and one territory that assessed the variations in privacy and security laws, organization practices, and policies that have an impact in electronic health information exchange—to maximize the impact of both HISPC and State Alliance efforts. The Taskforce conducted its meetings in a transparent manner, hosting them in public forums and hearing testimony from members of the public in these settings.

The Taskforce recognizes that its work is not yet done and will continue its examination of the issues around privacy and security in electronic health information exchange through this year. The Taskforce appreciates the State Alliance's consideration of this report and the recommendations it is advancing during this exciting period of tremendous change.

Sincerely,

William Hacker, MD

and

Sallie Hunt, JD

Health Information Protection Taskforce Co-Chairs

**MEMBERS OF THE HEALTH INFORMATION PROTECTION TASKFORCE
OF THE STATE ALLIANCE FOR E-HEALTH (2007-2008)**

Co-Chairs

William D. Hacker, MD, FAAP, CPE
Commissioner, Kentucky Department for
Public Health and Acting Undersecretary for
Health, Cabinet for Health and Family Svcs.

Sallie Hunt
Chief Privacy Officer
West Virginia Health Care Authority

Members

Holt Anderson
Executive Director
North Carolina Healthcare Information and
Communications Alliance, Inc.

Thomas W. Arnold
Deputy Secretary for Medicaid
Florida Agency for Health Care
Administration

Justin T. Barnes
VP of Marketing and Government Affairs
Greenway Medical Technologies, Inc.

Jim Bryant, PhD
Chief Information Officer
State of South Carolina

Jane Cheeks, JD, MPH
State AIDS Director
Alabama Division of HIV/AIDS Prevention
& Control

Bobbie Holm
Chief, Policy Branch
California Office of HIPAA Implementation

Kathy Hudson, Ph.D.
Director, Genetics & Public Policy Center,
and Associate Professor, Berman Institute of
Bioethics, Institute of Genetic Medicine,
Department of Pediatrics, Johns Hopkins
University

JoAnn Lamphere, DrPH
National Coordinator, State Health & LTC
Team
Government Relations and Advocacy
AARP

Scott Morgan
Natl. Privacy and Security Compliance Ofcr.
Kaiser Foundation Health Plan, Inc.
National Compliance, Ethics & Integrity
Office

Michele O'Connor, MPA, RHIA
Senior Director Healthcare Practice
Initiate Systems, Inc.

John Prestridge
Senior Manager, Industry & Technical
Marketing
Citrix Systems, Inc.

Alison Rein, MS
Senior Associate
AcademyHealth

Kristen Rosati, JD
Partner, Coppersmith Gordon Schermer &
Brockelman

Vera Rulon MS, RHIT, CCS
Director, Program Development &
Administration US External Medical Affairs
Chief Medical

W. Ob Soonthornsima
Senior Vice President and
Chief Information Officer
Blue Cross and Blue Shield of Louisiana

REPORT FROM THE HEALTH INFORMATION PROTECTION TASKFORCE TO THE STATE ALLIANCE FOR E-HEALTH

I. Introduction

The Health Information Protection Taskforce (“the Taskforce” hereafter) is charged by the State Alliance for e-Health with identifying and addressing issues pertaining to the privacy and security of consumer health information while allowing for seamless electronic health information exchange within and across states. Specifically the charge requires that the taskforce:

“Support the State Alliance for e-Health on issues regarding the protection of consumer health information that ensures appropriate interoperable, electronic health information exchange (eHIE) within states and across states. Develop and advance actionable policy statements, resolutions, and recommendations for referral to the State Alliance to inform their decision-making process in addressing state-level issues related to preserving the privacy of consumer health information while ensuring appropriate and secure electronic exchange of consumer health data within states and across states.”

In response to this charge, the Taskforce explored these issues through:

- 1) **Hearings and testimony:** The Taskforce conducted monthly meetings, beginning in February 2007, to explore state challenges to maintaining privacy and security of consumer health information in an eHIE environment. Over the past four months, the Taskforce members heard expert testimony from state representatives, privacy experts, individuals representing state HIE efforts, providers, public health, health information technology (health IT) leadership at the federal government, and individuals representing the consumer perspective.
- 2) **Work product analysis:** The State Alliance asked the Taskforce to conduct an analysis of how states handle the exchange of categories of data that typically have higher protections like mental health, HIV and other communicable diseases, genetics, substance use, and disability. The Taskforce has not yet completed this analysis and intends to present findings to the State Alliance in January 2008.
- 3) **HISPC analysis of variations and solutions:** Over the past year, 33 states and one territory participating in the Health Information Security and Privacy Collaboration (HISPC) assessed the variations in privacy and security laws, organization practices, and policies that have an impact in eHIE. Specifically, the HISPC states examined how various stakeholders, such as hospitals, physicians, insurers, and public health, implemented privacy and security policies and state laws at the practice-level given different scenarios in which data exchange may be necessitated.¹ The Taskforce examined the preliminary findings, summarized by RTI International on behalf of the HISPC states, to inform its initial exploration of the issues. Several of the Taskforce members also participate in the HISPC effort, which contributed to a desire by the Taskforce to continue tracking HISPC states’ progress to ensure coordination and maximize the impact of both efforts. In June 2007, the Taskforce convened a joint meeting with HISPC states to share lessons-learned and develop initial, consensus-based recommendations for privacy and security.

From the testimonies and deliberations noted above, the Taskforce identified findings, recommendations, as well as new Taskforce activities and products. This Taskforce Report presents the issues explored and recommendations for consideration by the State Alliance for e-Health to further advance, as guidance, to the states.

II. Current State of Privacy and Security in an Electronic Health Information Exchange Environment – Taskforce Findings

Sharing health data through the use of information technology in a seamless, electronic information network has the potential to improve health and health care. Availability of reliable health information at the point-of-care can enable physicians and patients to make better informed treatment decisions, can improve quality and efficiency of care, potentially lead to cost reductions, and save lives. At the same time, the prospect of storing, moving, and sharing health information in electronic form raises new challenges on how to best protect patient privacy and ensure data security. The Taskforce noted key findings that need to be addressed before interoperability within and across states can be realized.

Finding: State law consent requirements for the disclosure of health information vary within and across states, which may interfere with eHIE.

State privacy laws that govern information exchange have not kept up to pace with rapidly advancing technology. In many cases privacy requirements are scattered into different chapters of state legislation and regulation. Some are likely outdated or written for a paper-based system.² The result is a patchwork of requirements that may vary state-by-state and entity-to-entity, posing challenges to the interoperability of health IT systems and eHIE networks.

The complexity in the variation of state privacy laws is most evident in patient consent requirements, which impacts both inter- and intra-state exchange. State law consent³ requirements may vary by data type (e.g., general health, mental health, or HIV) and purpose of use (e.g., treatment, public health reporting, or payment). For example, in an interstate exchange where HIV data is needed for treatment purposes, some states require patient consent be obtained, while others do not require consent at all.⁴ States that do not have laws requiring consent for disclosure of information for treatment purposes defer to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), which allows covered entities to disclose protected health information for the purposes of treatment, payment, and health care operations.⁵

To add to the complexity, some state laws dictate specific requirements necessary for obtaining the consent. For example, if two states require consent, one might specifically require a written consent, while the other might allow for verbal consent. Specific requirements for obtaining consent are particularly inconsistent across states when it comes to the disclosure of data for categories of information that generally have higher protection (e.g., HIV, substance use, mental health, etc.).⁶ More specific scenarios demonstrating the potential challenges for interstate exchange associated with the variation in consent requirements between states are described below.

Scenario #1 - Variation in consent requirements to release health information to be used for treatment purposes: If one state requires a provider to obtain a signed consent to disclose health information to another provider in a different state in order to use the data for treatment of the same patient, the receiving provider may need to collect the consent from the consumer on a form

that complies with the sending providers' laws. This will require coordination between those providers, which takes time in a paper-based system. Moreover, if the sending provider must comply with a specific requirement like obtaining a "wet" (i.e., written as opposed to fax or verbal) signature to release the information, the receiving provider will require an in-person interaction with the consumer and may need to send the original, signed consent form to the sending provider. Absent consistent consent requirements, these types of interactions slow the transmission of health information that may be needed for timely and efficient care.

Scenario #2 – Variation in consent requirement for consumer participation in an eHIE:

The issue of exchange of information between health information exchanges—as is contemplated by the National Health Information Network—is slightly different. Consider the challenge posed by an "opt-out" model, where a consumer must object to being included from participation in an eHIE versus "opt-in" model, where the consumer must affirmatively consent to participating in the eHIE. If an eHIE in one state holds a consumer's information operating under an "opt-out" model, an eHIE in another state that requires a consumer to "opt-in" may not be able to receive that consumer's information without an affirmative contact with the consumer. Moreover, even if both eHIE follow an "opt-in" model, they may not be able to exchange information if they have different consent forms. For example, one eHIE may limit the consent obtained by time period or the purpose of the disclosure; this may not meet the requirements imposed on the other eHIE. In such circumstances, this would require a great deal of coordination between eHIEs and probable follow up with the consumer to exchange information.

At the intra-state level, consent requirements may be found in different chapters of the state legislation and regulation and potentially may be in conflict with each other, resulting in confusion of what exactly is required at the practice-level. According to the HISPC findings, health care entities' policies differ with respect to how the consent is required, obtained, documented, and communicated to non-related entities.⁷

The unevenness of consent requirements, exacerbated when scattered throughout state law, poses major challenges to the seamless flow of health data between entities within a state. The HISPC findings also suggest that whether varied within or across states, different consent requirements can be attributed to:

- Lack of standardized requirements for when consumer consent is necessary to disclose the consumer's health information (i.e. once, per instance when the data is accessed, or not alt all).
- Lack of a standard form to be used in connection with consumer consent.
- Multiplicity of approaches to the requirement for a consumer's information to be included in an HIE (i.e. opt-in, opt-out, or none).
- Variability in the accepted methods to validate consumer consent (i.e. email communication with consumer, faxed form, or "wet" signature).⁸

In addition to misaligned organization policies, the absence of consistent laws on consent has notable impact on the ability of the vendor community to set appropriate, standard security measures to ensure the protection of consumers' health information.

Finding: Health care entities use inconsistent security protocols for health data protection, which interferes with electronic exchange of health information.

Security protocols implement privacy protections and mitigate the possibility of inadvertent disclosures or inappropriate data use. Currently, health care entities approach the security of health data in different ways, which makes it difficult to identify clear security benchmarks. Inconsistent security protocols and lack of transparent benchmarks pose challenges to eHIE because of resulting mistrust among data source participants in an eHIE and concerns about potential liability. For example, one hospital considering participation in an eHIE may opt not to share data with another, competing hospital because it employs a different approach to securing health data or that its security approach is not transparent.

Challenges related to securing health data are found at two levels: (1) when data is at rest and (2) when data is in transit. Much of the Taskforce's discussion around security centered on "data in transit," specifically security challenges associated with exchanging health information between non-related entities, such as the exchange of health information between a hospital and independent physician practice. Through the testimonies, the Taskforce noted interconnected security issues that currently lack standardized approaches. These include:

- Accurately linking the correct individual (patient) with the correct health information.
- Authentication of individuals authorized to access protected health information.
- Mechanisms for ensuring the individual (e.g., provider) accessing patient data is authorized to do so.
- Information access controls to limit authorized individuals' access to the data that is appropriate for the individual's functions and needs.
- Auditing protocols that ensure coordination between entities to verify that only authorized individuals are appropriately accessing the health data and to identify possible breaches of security.

There are existing efforts at the national-level that aim, in part, to standardize security measures for eHIE. In an effort to achieve interoperability among the health information technology systems used by different health care organizations, the U.S. Department of Health and Human Services (HHS) supported the creation of the Health Information Technology Standards Panel (HITSP). HITSP's objective is to achieve widely accepted and readily-implemented consensus-based standards that will advance widespread interoperability among health information technology systems. HITSP identifies existing technical, interoperability standards and drafts implementation guides to ensure uniform implementation of these standards by different health information technology vendors. HITSP also identifies gaps in existing standards and notes standards not yet developed, but necessary for secure interoperability of systems.

As part of developing guides for uniform implementation of standards for interoperability, HITSP is identifying security standards for the areas mentioned above. One important note to consider, however, is that HITSP's activities are limited to use cases defined by the American Health Information Community (AHIC). AHIC functions as the advisory body to Secretary of HHS, Michael Leavitt, and the Department on all matters concerning the development of a Nationwide

Health Information Network. The use cases may not necessarily cover all aspects that are necessary to secure health data in circumstances not defined by the use cases. Furthermore, the use cases themselves may highlight the need for security and interoperability standards not yet available or developed.

A complementary effort supported by HHS is the Certification Commission for Health Information Technology (CCHIT). CCHIT is an independent, voluntary initiative that is charged with accelerating the adoption of health information technology by creating an efficient, credible and sustainable product certification program. As HITSP identifies standards and develops uniform implementation guides to enable secure interoperability, CCHIT facilitates the implementation of the standards through certification. It is a recognized certification body for certifying electronic health record (EHR) applications and eHIE networks. CCHIT has only developed certification criteria for in-patient and ambulatory EHR applications and, since the drafting of this report, has certified 90 EHR systems. It is currently developing criteria for network certification and may certify public health systems and electronic prescribing systems in the future.⁹

Despite the limitations noted above, both HITSP and CCHIT are complementary efforts that help address the security challenges identified by the Taskforce. HITSP identifies security standards that aid in enabling secure transmission of electronic health data between different entities, setting security benchmarks for eHIE. CCHIT helps implement the benchmarks by requiring EHR vendors to comply with security criteria for authentication, authorization, access control and audit in order to obtain certification.

Finding: Some federal privacy requirements pose implementation challenges for eHIE.

There are a number of federal laws that govern the privacy of health information. These include:

- The Health Insurance Portability and Accountability Act (HIPAA) and its Privacy Standards and Security Standards, 45 C.F.R. Part 160 and Part 164.
- 42 CFR Part 2 – regulations outlining requirements for the disclosure of information held by alcohol and drug-abuse treatment programs.
- Family Education Rights and Privacy Act of 2000 (FERPA) – privacy standards for school health records.
- Federal Medicaid Confidentiality Standards – privacy standards for use of Medicaid data.

Each federal law or regulation has different requirements for the protection of health data, some of which pose challenges to electronic health information exchange even for treatment purposes. For example, 42 CFR Part 2 (“Part 2” hereafter) applies to federally-assisted substance abuse treatment programs—providers for treatment of substance abuse. These regulations contain stringent protections and require providers to obtain written consent from the patient, using a specific form that meets requirements established by the regulation before disclosing information related to the patient receiving substance abuse treatment. This requirement applies to most types of disclosures, including for treatment in non-emergencies. Consent is required each time that the related health information would be disclosed, and must contain the following elements:

- Name or general designation of the program or person permitted to make the disclosure.
- Name or title of the individual or name of the organization to which disclosure is to be made.
- Name of the patient.
- Purpose of the disclosure.
- How much and what kind of information is to be disclosed.
- Signature of the patient (and in some States, a parent or guardian).
- Data on which the consent is signed.
- Statement that that consent is subject to revocation at any time except to the extent that the program has already acted on it.
- Date, event, or condition upon which consent will expire if not previously revoked.¹⁰

Part 2 also requires covered providers to append a written statement to the recipient of information (another provider), warning the recipient that the information is covered by these regulations and may not be released, as follows:

“This information has been disclosed to you from records protected by Federal confidentiality rules. The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.”¹¹

The Part 2 regulations pose challenges to substance abuse treatment providers—and other providers who receive Part 2-related information from them—in a few ways. First, because the regulations require patient consent for disclosure each time a disclosure is made, substance abuse-related data could not be shared in an eHIE for disclosures for non-emergency treatment without obtaining a written consent from the patient each time the information is needed. Since this disclosure prohibition applies to anyone who receives the patient’s information, it will essentially prohibit the inclusion of any substance abuse information from being included in an eHIE. Second, behavioral and mental health providers that treat patients in substance abuse programs report that it is difficult to segregate information regarding substance abuse treatment in their EHRs. In other words, providers are not able to parse out pieces of data in an individual’s medical record and manage substance abuse-related information differently. Oftentimes, the result is that behavioral health providers will not exchange any information with others without consent for each disclosure, and many will not participate in an eHIE. Third, the requirement to append a written statement to information released with consent may be difficult to implement in an eHIE environment.

In contrast to Part 2, the HIPAA Privacy Rule allows for the disclosure of health information when using the data for treatment, payment and health care operations. The exception to this rule is when the state privacy law is more protective. The HIPAA Privacy Rule only explicitly mandates authorization requirements for marketing purposes or the sharing of psychotherapy notes for purposes other than treatment.¹² It is also flexible in what it specifies as components for the consent and does not mandate that these components be implemented by entities covered under HIPAA.¹³

Another example of a different federal requirement posing challenges to eHIE is the Medicaid Confidential Data Standard, which restricts the use and disclosure of Medicaid data for applicants and recipients “to purposes directly connected with the administration of the plan.”¹⁴ Purposes directly related to the administration of the state Medicaid plan include:

- Establishing eligibility;
- Determining the amount of medical assistance;
- Providing services for recipients; and
- Conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of the plan.¹⁵

The federal Medicaid Confidentiality Data Standard specifies that information such as medical data, including diagnosis and past history of disease or disability; and medical services provided to Medicaid beneficiaries be safeguarded from being disclosed for purposes other than what is listed above.¹⁶ The federal Medicaid Confidentiality Data Standard requires that permission from a family or individual be obtained prior to responding to a request for information from an outside source.¹⁷ These provisions do not lend themselves to allowing for the release of Medicaid information for eHIE in certain circumstances, like electronic prescribing (ePrescribing). ePrescribing, conducted through a computer or a handheld device, enables physicians to electronically generate and submit prescriptions directly to a pharmacist. It also can make available current drug list, medication history, formulary, and eligibility information to physicians and pharmacies for preventing adverse drug interactions and fraud and monitoring patient medication compliance. There is uncertainty at the state-level about whether using Medicaid information for ePrescribing purposes is allowable under the current Medicaid rules.

The different requirements and complexities of federal laws and regulations lead to confusion and compliance challenges at the practice-level. The interaction between FERPA, HIPAA and Part 2, for example, demonstrates the complexities of complying with these laws and regulations for electronic health information exchange.

Student health records maintained by an educational agency or institution or by a person acting for such agency or institution are covered by FERPA.¹⁸ FERPA requires that consent from the student (or the student's parents if the student is minor) before release of that information in many circumstances. The HIPAA Privacy Rule also covers schools, colleges, and universities, if they function as health care providers that engage in HIPAA standard transactions (like electronic claims submission), but allows for exchange of information for treatment purposes.¹⁹ The Part 2 regulations apply to school-based health records generated by any student assistance programs that “specialize, in whole or in part, in providing treatment, counseling, or assessment and referral services for students with alcohol or drug abuse problems.”²⁰ However, as noted earlier, Part 2 regulations require a specified consent prior to release of information even for treatment purposes. The rules of disclosure of health information in these three sets of regulations are different and their interaction is very confusing for school health programs.

The different requirements for disclosure of health information found in various federal privacy laws cause confusion among providers about what exactly is required. This challenge is compounded when coupled with the complexities of state privacy laws. Moreover, some federal privacy laws like FERPA and Part 2, when addressed in isolation, are onerous to implement technologically and at the practice-level. The impact of the different requirements is that

providers often do one of three things—none of which promote good patient care or protect the patient from harm:

- 1) Leave the data (if subject to specific, arduous requirements) out of the exchange and rely on patient recall;
- 2) Simply disregard the information; or
- 3) Apply the most stringent requirement for all types of data that make up the health record.

In addition to the intricacies of federal privacy laws, the interaction between the range of federal and state privacy law requirements make true compliance to all that apply at the practice-level complex. The impact of this variation also applies to the technology systems. The Taskforce learned that mapping multiple, yet variable policies to technical standards for capturing consent electronically would be arduous and infeasible to cross-state, inter-entity health information exchange.

III. Policy Statements

In light of the current state of the privacy and security challenges to eHIE, the Taskforce offers the following policy statements and recommendations.

Policy Statement: States need a framework to help guide their individual efforts and facilitate a coordinated approach to privacy and security challenges related to eHIE.

The Taskforce members recognized early on in their deliberations that states need a cohesive lens through which to examine and organize the breadth and complexity of privacy and security challenges to eHIE. The Taskforce heard testimonies from states that were undergoing the process of reviewing existing privacy laws and noted frustration in the uncertainty of where to begin and how to best tackle the issues. The Taskforce, itself, expressed similar concerns when trying to narrow its scope of work for this year and identify the appropriate approach to its work product.

The critical security challenges to eHIE are not technical. They are driven mostly by policy uncertainties on how to handle privacy of health information in an exchange. The Taskforce, therefore, explored privacy frameworks developed by reputable collaborative efforts and identified common privacy elements that may be offered to states as a starting point. The collaborative efforts explored by the Taskforce include:

- *Common Framework Privacy Principles* – developed by the Markle Foundation’s Connecting for Health Collaborative, composed of leaders from more than 100 public, private, and not-for-profit organizations including those representing employers, physicians, hospitals, research institutions, health policy organizations, system integrators, and vendors. The Common Framework Privacy Principles outlines nine elements derived from the Fair Information Practices Act and the European Union Privacy Principles and translated in the eHIE context.²¹ A number of states, including Utah, Colorado, Minnesota, and Oregon, have used the Common Framework Privacy Principles to help guide their thinking about these issues.²² Some states did provide feedback, however, that the Common Framework Privacy

- *Analysis of Privacy Principles: An Operational Study* – developed by the International Security Trust and Privacy Alliance (ISTPA), a global alliance of companies, institutions, and expert practitioners working together to address broad privacy-related operational issues, not solely within health care. The ISTPA analyzed principles embedded in 11 different frameworks recognized in the privacy community. These ranged from United States’ privacy laws like the Privacy Act of 1974, Fair Information Practices Act, and HIPAA to international guidelines like the Organisation for Economic Co-Operation and Development (OECD) Privacy Guidelines, UN Guidelines Concerning Computerized Personal Data, and Canadian Standards Privacy Code.²³
- *Consumer Principles for Health IT* – developed and endorsed by more than 20 consumer and privacy advocacy organizations including the National Partnership for Women and Families, AFL-CIO, Consumers Union, Health Care for All, and Health Privacy Project. The Consumer Principles for Health IT outlines seven principles that emphasize consumers’ rights in eHIE.²⁴

The Taskforce compared the principles from these collaborative efforts and identified common elements from each. The Taskforce believes that these elements should be considered when states are developing or altering privacy laws, regulations, and policies for eHIE. These elements include:

- | | |
|---|--|
| <ul style="list-style-type: none"> • Accountability for ensuring privacy and security compliance, enforcement of compliance, and remedies to individuals for breaches • Purpose for data collection and collection limitations • Consent process • Consumer education • Data quality • Disclosure of health information | <ul style="list-style-type: none"> • Health care quality and quality measurement • Individuals’ Rights • Security safeguards for protecting data from unauthorized access, destruction, and improper use • Notice to individuals regarding privacy policies • Openness regarding development of privacy policies • Limitations for intended uses of the data |
|---|--|

The Taskforce offers these elements as well as considerations or questions that states may utilize as they develop privacy laws, regulations, and policies for eHIE (see Appendix A). For example, when developing a privacy policy or regulation, states may incorporate a provision related to the data quality element. When crafting the language, states may consider the following questions with respect to data quality:

- How are the data kept accurate, relevant, and time stamped?

- Is the information collected and used and disclosed adequate for the purpose identified?
- Where necessary, how are data amended and sequestered?
- Is there a method for accurately identifying the individual in the system? Across systems?
- Is the data verifiable at the point of use?
- Does the data maintain the identity of the originator and date of origination?
- Are there mechanisms to maintain the data quality while in transit?

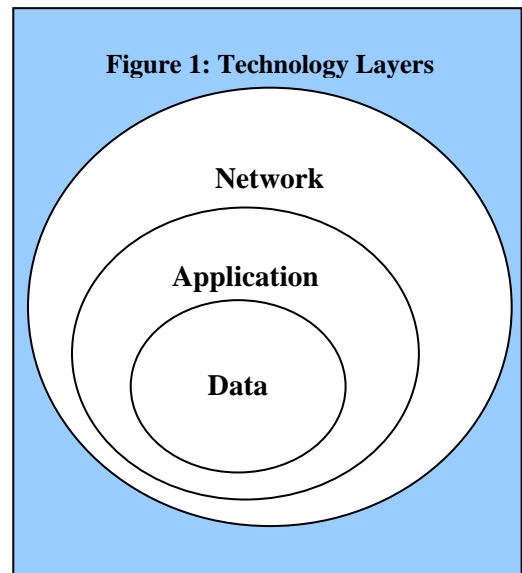
The Taskforce recognizes that these privacy elements and considerations may not be all encompassing, but offers them to the State Alliance and states as a starting point when revising or creating privacy laws and policies. The Taskforce is pleased to learn that the Office of the National Coordinator for Health IT within the U.S. Department of Health and Human Services is developing a framework for privacy that will be vetted with various stakeholders in the near future.

The Taskforce also notes that further guidance to states with respect to the appropriate vehicle by which they may address these elements is needed. Providing states, for example, with guidance relative to which elements may require legislation versus what can be accomplished through regulation or policy would be helpful. Fitting certain elements into the legislation bucket, versus regulation or policy remains a challenge. The Taskforce offers the State Alliance and states one methodology, outlined in Appendix B.1 and B.2, which may help states make these determinations.

Policy Statement: As states develop networks for exchange of health information, privacy and security policies must be developed in concert with the technical architecture of the eHIE.

In almost every testimony heard by the Taskforce, speakers noted the importance of recognizing how policy and technology are closely intertwined. As one speaker commented, “Choices about one necessarily shape the other.”²⁵ Both must support each other’s development and remain flexible to allow each to continue evolving. The Taskforce recognizes that technology advancement should not be stunted by overly restrictive policies. Similarly, technology built should not limit policy choices. Policy decisions will naturally continue to evolve as we get more innovative with eHIE and discover new necessities to protect consumers.

Privacy and security policies should be developed in concert with the technology, and enveloped at every layer of technology in an eHIE. These layers are: (1) data, (2)



application, and (3) network (Figure 1). For example, when building the network technology for exchange of information, states should simultaneously work to address policy issues related to secure transmission of the data. The table below showcases some example considerations for technology and policy to simultaneously address when developing an eHIE.

Technology Layer	Example Technology Considerations	Example Privacy and Security Policy Considerations
Data	<ul style="list-style-type: none"> ➤ How do you provide strong authentication for authorization of access to health data? 	<ul style="list-style-type: none"> ➤ Who should be provided access to what type of data (role-based access)? What are the policies required to protect data from unauthorized access of information? ➤ How is data protected when at rest?
Application	<ul style="list-style-type: none"> ➤ What are the desired functionalities from the software application that will host/store the data? Do the desired functionalities accommodate the defined purposes and uses of the data? ➤ How are applications and databases protected from unauthorized access? 	<ul style="list-style-type: none"> ➤ What are the purposes and uses of data hosted/stored in the application? ➤ What IT security policies are required to ensure privacy of health data collected in the applications? Have appropriate access controls been defined and implemented? Is there an audit log policy and does the technology have the capability to implement that policy?
Network	<ul style="list-style-type: none"> ➤ What are the standards that will allow for different applications to be connected electronically so that data can flow seamlessly in a network? ➤ How is data protected when being transmitted over public-wide area networks? 	<ul style="list-style-type: none"> ➤ What are the security policies for handling data in transit within the entity? Between entities? Across states?

Delicately balancing technology and policy development is necessary if successful eHIE is to be achieved and if the public's trust is to be gained. Furthermore, the integration of policy discussions with technology is necessary to optimize the value of any eHIE effort for the community at large.

Policy Statement: Consumers should be informed and engaged in discussions about the extent to which their health information is protected in an exchange environment. They also should be informed about the potential benefits of, and their roles and responsibilities in, an eHIE environment.

Considerations for consumers have been central throughout the deliberations of the Taskforce since its first meeting in February 2007. The Taskforce heard from experts and fellow members how critical it is to ensure that consumer protections are considered when developing policies and strategies for technology interoperability in eHIE. Similarly, the Taskforce identified consumers as important stakeholders of any health information exchange effort. Members and experts noted that consumers should be engaged in discussions about privacy and security and the potential benefits of eHIE early on in the process of building the electronic exchange environment. Consumer engagement is critical to gaining public trust. Without trust of the public, the eHIE effort may fail.

Experts expressed, however, the challenges associated with engaging consumers. The primary challenge is getting the consumers to the discussion table. There is no apparent way for eHIE efforts to include the consumer perspective in discussions. Consumers are not represented in

totality as a group in the same way as other stakeholders in health care come together. For example, physicians have specialty and state societies, as well as national associations to represent their viewpoints. Hospitals, too, have an umbrella association that can truly speak on behalf of their interests. The same can be said for health plans. Consumers, on the other hand, have no single appointed entity to act on their behalf.

Some consumers' interests are represented through a disease-specific advocacy organization, employee union, or other topically-based advocacy organization. Privacy advocates also represent consumer interests. The Taskforce recognizes that advocates' representing consumer viewpoints have been absolutely essential to eHIE efforts. Reaching out to consumer and privacy advocacy organizations is one approach to having the necessary consumer perspective represented in decision-making processes about eHIE policies. However, advocacy organizations are also challenged in their efforts to represent the consumer viewpoint. eHIE is a highly complex issue that requires some knowledge of law, technology, and the health care sector. This level of knowledge is rarely found in consumer organizations, and needs to be cultivated to ensure informed, appropriate and active consumer participation.

Discussions about consumers and eHIE emphasize placing the control of information exchange at the hands of individual consumers, which include individuals who are not always represented by an advocacy organization. For example, a 30 year-old healthy female would most likely not be represented by a consumer advocacy organization. As eHIEs mature, it will be critical to engage both consumer advocates and individual consumers themselves.

A lesson-learned from the testimonies heard by the Taskforce with respect to consumer engagement is the usefulness of interviews and focus group approaches to more directly reach individuals and obtain their perspectives on eHIE. The Taskforce heard from state representatives from Michigan, Rhode Island, and Oregon. These states conducted detailed interviews or focus group sessions of consumers to gauge their knowledge and attitudes about health IT, eHIE and privacy, as well as to identify their concerns and preferences. By directly reaching out to individual consumers, these states were able to incorporate consumer viewpoints and preferences in the state's policy-development process for eHIE.²⁶ As states increasingly use interview and focus groups approaches, however, a rigorous methodological approach for evaluating consumer awareness and preferences with respect to eHIE is necessary. The Taskforce may address this when developing the consumer communication tool noted in the recommendations section below.

IV. Recommendations

In addition to the policy statements noted above, the Taskforce identified recommendations specific to addressing some of the challenges outlined in previous sections of this report that are related to technical security and the coordination of state and federal privacy requirements. The Taskforce jointly crafted these recommendations with the HISPC states that met with the Taskforce members in June 2007. Twenty-six of the 34 HISPC states were able to attend the meeting.

Taskforce Recommendations on Technical Security

To bring some level of standardization to security measures for authentication, authorization, access controls, and audit, the Taskforce advances the following recommendations to the State Alliance for consideration.

Recommendation 1.0: The State Alliance should encourage states to recognize the certification of newly acquired electronic health record (EHR) applications and network components by the Certification Commission for Health Information Technology (CCHIT) or other certification body designated by the Secretary of the U.S. Department of Health and Human Services. One method states could consider is to require, that as part of participation in publicly funded programs, any provider that engages in electronic health information exchange when using newly acquired products or network components, should use a product or network that meets the certification process recognized above.

The Taskforce believes that this recommendation will help on two fronts. First, the certification of EHR applications and network components will ensure that well-vetted security standards are implemented and that the technologies will continue to meet higher security benchmarks as certification requirements advance each year. Second, certification is intended to assure providers that the systems they purchase are – to the extent possible at the time – interoperable and include the latest security standards.

A system that has passed CCHIT requirements represents the state of the art in capabilities known in that certification year. It would not, however, be considered interoperable or secure in perpetuity. CCHIT will continue to set higher security benchmarks in its certification requirements, and vendors are expected to bring improved systems to CCHIT periodically for certification against these newer, enhanced criteria and standards. The CCHIT certification seal is valid for up to three years from the original date that the certification was obtained. The three-year timeframe takes into consideration the product development cycle of health IT systems. Moreover, the seal is marked with the original certification year, so purchasers always know when the certification was obtained²⁷

The Taskforce also would like to clarify a few additional points for states to bear in mind with respect to Recommendation 1.0:

- When setting policy on certification requirements for participation in publicly-funded programs, states should be flexible and give health care organizations sufficient time to migrate to certified EHR projects without penalty or substantial expense. For example, organizations that are very large and complex, such as major medical centers, will need more time than one year to transition. In this case, states may provide greater flexibility on the time required to obtain valid certification. In contrast, smaller settings like physician practices have less complex systems and may be able to upgrade current systems more easily. Often, physicians who purchase EHR applications also purchase on-going maintenance support from the vendors that may enable such upgrades.
- Certification requirements should recognize the efforts already made by health systems using homegrown or legacy systems that have been able to successfully exchange electronically within their closed networks. Certification should not penalize these early adopters by setting a certification requirement that would place

an unreasonable condition on their participation in publicly-funded programs. Instead, efforts should be made to help them move towards certification and interoperability. One approach states may consider is to provide incentives for these systems to map existing capabilities with those required by the certification process in order to identify gaps. States can then determine a phased-in approach over several years depending on the complexity of the gaps that still moves these systems toward meeting certification standards and interoperability.

- States should also take into account the product development cycle of software and network applications when developing policies related to certification. EHR applications typically have a two to three year development cycle. However, more complex applications may have longer development cycles. Certification requirements should encourage innovation and competition, but not without consideration for equitable, realistic expectations of the vendor community.

Recommendation 1.1: The State Alliance should encourage the President to call on the Secretary of the U.S. Department of Health and Human Services to designate a single, national certification body (such as CCHIT) for use by all relevant federal agencies, and require product and network certification for participants in all federally funded programs, grants, and contracts for newly acquired products or network components.²⁸

Although HHS supports the efforts of CCHIT, it has yet to formally designate a single, national body for the certification of recognized interoperability standards for health IT systems and networks. President George W. Bush's Executive Order 13410 leaves the definition of recognized interoperability standards to the Secretary of HHS.²⁹ States understand the need to have a formalized certification process in order to ensure that systems are secure and meet recognized interoperability standards and therefore call on the Secretary to formally designate a certification body. Currently, no other certification body currently exists besides CCHIT.

The Taskforce recognizes that CCHIT is a fairly new effort that is still evolving and growing into its role. However, it has gained the support of stakeholders in the vendor community as well as health IT users. It has a transparent, deliberative process and is mindful of the implementation challenges associated with seeking certification. If the federal government does not intend to formally designate CCHIT as the certification body for health IT systems and networks, then it should identify another and give its formal approbation to avoid significant and costly changes that may be incurred by all eHIE stakeholders, including itself. States efforts to further the development of secure eHIE through certification policies that incorporate CCHIT requirements will be frustrated if the federal government does not apply the same standard to its programs. Simply supporting the effort does not go far enough to assertively driving change and the transition of these systems towards enabling secure, interoperable eHIE.

The Taskforce also would like to emphasize that the same points made in Recommendation 1.0 with respect to health system complexities, legacy information systems, and product development cycles apply as well to Recommendation 1.1.

Recommendation 1.2: The State Alliance should encourage states to become engaged and provide input into the certification process by supporting the participation of State Chief Information Officers (CIOs), public program CIOs and state health IT coordinators (or equivalent-level personnel) in the CCHIT, HITSP, or similar federally-endorsed activities in order to ensure that the state perspective is incorporated, and to ensure applicability of the requirements in the state environment.

The Taskforce members noted that the participation of states in these standard-setting processes is critical to ensuring that they are applicable to and considerate of states' unique environments. Both the CCHIT and HITSP efforts, for example, are public-private activities and encourage participation by various stakeholders including state government representatives with health IT implementation experience. State government representatives can join and contribute to the various work group activities in each process. States, in general, should keep track of national-level health IT and eHIE activities and provide input to these efforts as appropriate.

Recommendations on Reducing Variability of State and Federal Privacy Environments

The current landscape of state and federal laws and regulations governing privacy of health information poses challenges to the timely and efficient electronic health information among members of the health and care community. In light of the context previously outlined, the Taskforce forwards the following recommendation to the State Alliance for consideration.

Recommendation 2.0: The State Alliance should encourage states to continue to (1) educate leaders of the executive and legislative branches on the importance of interstate alignment of privacy protections and (2) sustain efforts through financial and political support or other means, to reduce the variability of state privacy requirements within and across states, in a manner that ensures appropriate consumer protections are in place.

The success of state efforts to develop in this arena will be limited by some federal privacy requirements that pose challenges to eHIE. The variability of existing federal requirements related to privacy of health information is in conflict with the stated vision of achieving interoperable, electronic health information exchange in the United States. As previously noted, the federal requirements related to the implementation of the consent process for substance abuse and student health information vary significantly from what HIPAA requires. The conflict between the federal requirements and the stated vision may pose barriers to achieving the goals of enhancing care quality, improving patient safety, and reducing system costs through integrated health information flow.

As such, the federal government should also undergo a review of its privacy requirements in a similar manner that the states have undertaken through the Health Information Security and Privacy Collaboration effort. It should examine federal statutory requirements related to the privacy of health information that poses challenges to eHIE, while maintaining appropriate consumer protections. In light of this context, the Taskforce proposes the following recommendation for consideration by the State Alliance.

Recommendation 2.1: The State Alliance should call on the Executive Branch of the federal government to work with the Alliance to identify challenges in current federal statutory and regulatory requirements (such as HIPAA, FERPA, 45 CFR Part 2, Federal Medicaid regulations, CLIA, etc.) and create mutually acceptable solutions that would allow for alignment of these requirements as they relate to the privacy and security of health information and health information exchange.

During a joint meeting with the HISPC states in June 2007, the Taskforce identified current regulatory frameworks that create challenges for eHIE. Some of these regulatory frameworks were discussed in the findings section of this report. The Taskforce's discussions displayed a

clear understanding of the original intent of these regulations, but stressed that much of that policy was developed prior to eHIE, and even prior to HIPAA. The Taskforce encourages the federal government to work with states to develop appropriate federal standards to protect health information and encourage eHIE.

V. Health Information Protection Taskforce Next Steps

Working under its current charge, the Taskforce will continue to investigate privacy and security issues in eHIE over the next several months in 2007. The Taskforce will focus its efforts on addressing challenges related to the implementation of consent requirements across states, safe harbors for providers, and consumer education.

Taskforce Action: Consent Content and Process Options

In light of the challenges posed by the variability of state privacy requirements and the need to modernize the implementation of the consent process to accommodate for an environment of electronic health data sharing, the Taskforce will:

- 1) Develop essential definitions pertaining to patient consent for health information exchange in an electronic environment
- 2) Develop consent content and process options to securely enable interstate, electronic health information exchange.

Taskforce Action: Safe Harbor Language for Providers in eHIE

Throughout its deliberations, the Taskforce was cognizant of provider concerns about the potential liabilities associated with eHIE. Uncertainties about the potential risks in an electronic environment have posed significant barriers to widespread adoption and use of health IT systems by providers. Widespread adoption and use of these systems is a necessary component of achieving eHIE. To address the challenge of unknown liability and provide appropriate measures to mitigate risks to provider investment in these systems and encourage participation in eHIE efforts, the Taskforce will develop model safe harbor language limited to protecting providers in the exchange of information for treatment purposes when reasonable representations and authentications are presented and when the exchange is made in good faith. The model safe harbor language may be used as guidance for states to consider when developing legislation supportive of eHIE.

Taskforce Action: Consumer Awareness and Communication Tool

The Taskforce recognizes that public trust is a critical component to enabling interoperable eHIE. Raising consumer awareness about the purpose and potential value of eHIE is a necessary step to gaining public trust. States, as protectors of the public's health, are committed to finding ways to ensure that consumers are engaged in the discussions regarding their health care. In the privacy context, consumers are not fully aware of their privacy rights or the value eHIE brings to improving the quality of their care and enhancing their safety. They are not fully aware of the benefits of eHIE to helping them better monitor their health data and make better informed decisions with their providers.

At the same time, the Taskforce knows of the challenges associated with engaging lay consumers in discussions about the privacy of their health information in an eHIE. There is uncertainty on what messages to communicate, how much information is necessary to communicate that won't overwhelm the consumer, and what appropriate communication vehicles exist for raising awareness. Moreover, as previously noted, consumer advocates also need resources to support their efforts to engage individual consumers. The Taskforce will continue to investigate this issue and work towards identifying best practices in risk and benefit communication to offer as guidance to states.

Appendix A. Considerations for Each Element Relating to Privacy Policies for Electronic Health Information Exchange

Privacy Policy Element	Element Considerations
Accountability, Enforcement, and Remedies	<p>Accountability</p> <ul style="list-style-type: none"> • Who monitors compliance with privacy and security policies? • Who is responsible for compliance? • Are individuals involved in governance of a health information exchange? • How are affected individuals informed about privacy violations and breaches? <p>Enforcement</p> <ul style="list-style-type: none"> • What are the mechanisms to ensure compliance with privacy policies, agreements and legal requirements? • Who is responsible for enforcement? <p>Remedies</p> <ul style="list-style-type: none"> • How will individual complaints be handled (in what manner/time frame)? • Are there legal or financial remedies in the event of a breach?
Collection Purpose and Collection Limitation	<p>Purpose specification</p> <ul style="list-style-type: none"> • Have the purposes for the data collection been completely enumerated? • Have the purposes been completely and clearly defined? <p>Limitation</p> <ul style="list-style-type: none"> • Do the constraints exercised by the data collector and user to limit the information collected still allows for the stated purpose to be achieved and when required demonstrably collected by fair and lawful means? • Is the information complete? If not, will its absence (potentially) impact quality and patient safety?
Consent	<ul style="list-style-type: none"> • Has a decision been made about which consent process is required? If so, has a decision been made about which consent is to be applied (opt-in or opt-out)? • Is there a consent process to support exchange of health information and change of use consent? • Are the consequences of consent denial provided to the patients to allow the collection and/or specific uses of

Privacy Policy Element	Element Considerations
	<p>some or all of their personal data?</p> <ul style="list-style-type: none"> Is there a process to inform the consumer and obtain the consent of the consumer for the release, transfer, provision of access to, and use for new purposes or divulging in any other manner of the information held by the entity?
Data Quality	<ul style="list-style-type: none"> How are the data kept accurate, relevant, and time stamped? Is the information collected and used and disclosed adequate for the purpose identified? Where necessary, how are data amended and sequestered? Is there a method for accurately identifying the individual in the system? Across systems? Is the data verifiable at the point of use? Does the data maintain the identity of the originator and date of origination? Are there mechanisms to maintain the data quality while in transit?
Disclosure	<ul style="list-style-type: none"> Can an individual find out what data has been collected? Does the process include the tracking and audit trail systems? Is the policy of the entity regarding disclosures understandable and state who can access the data and ways in which the data can be used or shared? Are the data collector's policies known to and observed by third parties receiving the information (under contractual relationships)? Or are there limitations for re-disclosure by third parties?
Education	<ul style="list-style-type: none"> Is there an accompanying consumer education program available for individuals, so that people understand how the network will operate, what information will and will not be available on the network, the value of the network, its privacy and security protections, how to participate in it, and the rights, benefits and remedies afforded to them.
Health Care Quality and Quality Measurement	<ul style="list-style-type: none"> Is it supportive of quality measurement, provider and institutional performance assessment, relative effectiveness and outcomes research, prescription drug monitoring, patient safety, public health, informed decision-making by patients and other public interest objectives, while protecting patient privacy?

Privacy Policy Element	Element Considerations
Individuals' Rights	<p>Access related to the individual (patient) or personal representative</p> <ul style="list-style-type: none"> • Do individuals have access to all of their personally identifiable information in a convenient and affordable manner? • Do individuals have the ability to supplement, request correction of, and share their information without unreasonable fees or burdens? • Do individuals have access to who has accessed their information? • Is there a method for appropriately authenticating individual's or their personal representative's access? (Authentication and credentialing) • Is there a method for verifying the identity and relationship of the personal representative? • Are the notice of denial for access and options for challenging denial provided to individuals in a clear and understandable manner? <p>Access related to the health care provider (provider = both individuals and institutions)</p> <ul style="list-style-type: none"> • Is there a method for verifying the identity of the provider accessing the patient's information?
Security/Safeguards	<ul style="list-style-type: none"> • How are the data secured against breaches? • Is there a mechanism for tracking and monitoring for possible breaches? • How are the data secured against destruction and improper use? • How are the data secured against loss? • How are the data secured against unauthorized access? • Is there a mechanism for timely notification of individuals in the event of breach? • How is the public informed about privacy violations and breaches? • Is there a business continuity and disaster recovery plan to avoid "down-time" and backup to avoid "fail-over"?
Notice	<ul style="list-style-type: none"> • Is there a notification process? • Does the notice include information about the entity's privacy policies and practices regarding: <ul style="list-style-type: none"> ○ definition of the personal information collected; ○ reason(s) for collection (purpose specification); ○ its disclosure of information to parties external to the entity; ○ practices associated with the maintenance and protection of the information; ○ options available to the data subject regarding the collector's privacy practices;

Privacy Policy Element	Element Considerations
	<ul style="list-style-type: none"> ○ changes made to policies or practices; and ○ how an individual can get their own information?
Openness	<ul style="list-style-type: none"> • Is it easy to understand what policies are in place, how they were determined, and how to make inquiries or comment? • Is it clear who has access to what information for what purpose? • Are individual's rights clearly articulated or communicated?
Use Limitation	<ul style="list-style-type: none"> • Will the data only be used for the purposes stated? • If consent was required, was the purpose stated agreed to by the subjects? • Does the consumer have control over whether, how, and with whom the information is shared?

APPENDIX B.1: WORK PRODUCT RESEARCH METHODOLOGY **INTEGRATION OF POLICY, LEGAL AND HIT PROCESSES** **FLOW DESCRIPTION (also refer to Appendix B.2 when reviewing)**

Overarching Criteria for Analysis Process

1. *Adopt a Privacy and Security Framework.* Prior to beginning a process to analyze issues a framework (principles) should be adopted against which potential solutions will be tested. A sample framework may be based on the Connecting for Health Network framework or the International Security Trust and Privacy Alliance (ISTPA) framework. .
2. *Develop Generic Alternatives for Each Aspect.* Develop a listing of potential alternatives that may be considered for social driver solutions, legal solutions, business process solutions, and technical solutions. This may include such things for legal as proposed law change, model state law, contract language, consensus agreement on an interpretation of a statute or regulation.
3. *Develop Criteria to Evaluate Each Alternative.* Develop criteria to be utilized to evaluate the effectiveness of each alternative. The criteria may include economic impact, legal impact, stakeholder impact, consumer impact, etc.
4. *Develop a Process and Criteria to Select the Issue to be Analyzed.* A process needs to be adopted to identify and prioritize the issues that will be analyzed. This process may include decision box 4 which would determine if the prospective issue identified could be addressed by a broader solution, e.g., a decision to adopt opting in with informed consent could include a consent form incorporating authorizations to allow sensitive data be exchanged. Establishing additional criteria would provide for a more a deliberative selection process.
5. *Select Issue to be Analyzed.* Utilizing the selection process and its criteria, select the issue to be analyzed.
6. *Select the States and Businesses to be Analyzed:* Select the states and businesses whose social drivers, laws, business processes and/or technical standards, systems, or architecture will be reviewed during the analysis of the issue.

Background Development

7. *Define: Scope (Treatment), Assumptions and Constraints.* There are some assumptions that, if made, may change the results of the analysis. If this process assumes that HIE will only exchange information for treatment, decisions may be different than if the process assumes that all permitted disclosures under HIPAA will be allowed. For example, the process could limit the exchange to treatment or

extend the exchange to public health, homeland security, and research, thus affecting access issues. Other types of assumptions are: 1) HIPAA will be the baseline standards for data in an HIE, 2) consumers be required to opt into HIE through informed consent, etc.

8. *Will the Issue be Resolved through Solutions to Broader Issues?* This box may be part of the process for selecting an issue or may be necessary at this stage of the process, but somewhere, and may at a few different times during the process this question should be asked.
9. *Identify Which of These Contributes to the Issue Barrier: Social Drivers, Laws, Business Practices, Technology*
 - Collect Data and Analyze Social Drivers
 - Collect Data and Analyze Law
 - Collect Data and Analyze Business Processes
 - Collect Data and Analyze Technical Systems and Architecture

This is the portion of the process that research begins and data is collected to determine if the issue is caused by social drivers, law, business processes, or IT systems. An issue may have several causes and need to be processed through more than one of the types of analyses.

	Social Drivers	Law	Business Processes	Technical Systems
10.	<i>Collect Data and Analyze Social Drivers:</i> Research the background of the issue. Review the public law, legislative history, legislative intent, related court cases, current and potential HIT implementations, eHIE architecture being used or proposed, and any other pertinent background information. Examine the issue to determine if the cause of the issue is social drivers. Determine if the social drivers	<i>Collect Data and Analyze Law:</i> Research the background of the issue. Review the public law, legislative history, legislative intent, related court cases, current and potential HIT implementations, eHIE architecture being used or proposed, and any other pertinent background information. Examine the issue to determine if the cause is law. Determine if the law remains pertinent, what is the intent of	<i>Collect Data & Analyze Business Processes:</i> Research the background of the issue. Review the public law, legislative history, legislative intent, related court cases, current and potential HIT implementations, eHIE architecture being used or proposed, and any other pertinent background information. Examine the issue to determine if the cause is business processes. Determine the source or driver of the	<i>Collect Data and Analyze Technical Systems:</i> Research the background of the issue. Review the public law, legislative history, legislative intent, related court cases, current and potential HIT implementations, eHIE architecture being used or proposed, and any other pertinent background information. Examine the issue to determine if the cause is technical. Determine the purpose of the technical cause.

	Social Drivers	Law	Business Processes	Technical Systems
	remain pertinent.	the law, is it the result of social drivers.	processes. Does the result of the process remain pertinent?	Does it remain pertinent?
11.	<i>Identify and Engage Affected Stakeholders:</i> Provide the background research for discussion with affected stakeholders. Determine from their input which solution may be the best to pursue through the process. There may be a recommendation that more than one solution may exist. Document the input.			
12.	<i>Determine How Social Drivers Affect the Issue:</i> Determine how the social drivers impact the issue, do they stop the exchange of the information, or only influence the method in which it is exchanged?	<i>Identify Laws Affecting the Issue:</i> Identify the laws that apply to the privacy and security for the issue in the states selected. Should this include regulations? State laws only, no federal laws? How about local ordinances or entity policies and procedures? There may be more than one driver for a law.	<i>Identify Business Practices Affecting the Issue:</i> Identify the business practices that apply to the privacy and security for the issue in businesses selected in the states selected. What drives the business practice; law, regulations, policies, local ordinances, other?	<i>Identify Technical Standards Affecting the Issue:</i> Identify what technical standards, systems, or architecture affects the privacy and security of the medical information for the businesses selected in the state selected
13.	<i>Determine the Validity of the Social Driver:</i> Is the social driver still pertinent in the state selected? Has the situation changed in a way that the law may no longer be necessary? Have other social drivers evolved to support the law?	<i>Determine the Validity of the Law:</i> Is the purpose of the law still being met? Does the problem of the law was intended to address exist?	<i>Determine the Validity of the Business Process:</i> Determine if the business process meets its original purpose. Does the original purpose continue to exist?	<i>Determine the Validity of the Technical Standard, System, or Architecture:</i> Determine if the technical standard remains necessary. Does it continue to meet the original purpose? Does the original purpose continue to exist? Does the system or architecture need to be updated? At what cost?
14.	<i>Identify Countervailing Social Drivers:</i> Are there countervailing social drivers? Do these drivers indicate a	<i>Identify the Countervailing Laws:</i> Are there countervailing laws? Do these laws indicate a needed change? Are the laws	<i>Identify How Business Processes Affect the Issue:</i> Determine how the issue is affected by the business process. Does it stop	<i>Identify How the Technical Standards, System or Architecture Affect the Issue:</i> Determine how the IT affects the

	Social Drivers	Law	Business Processes	Technical Systems
	needed change?	preempted by the countervailing law?	the exchange, delay, or require additional administrative activities before the exchange occurs?	issue. Is the original purpose of the IT standard, system or architecture continue to exist and/or be met? Does it need to be changed?
15.	<i>Do Social Drivers, Laws, Business Process or HIT Support Each Other?</i> Determine if the relationships exist between the social drivers, the laws, business process and HIT design. Determine if there is a support relationship between these items. Do the relationships continue to be valid or do they need to change? Is there a relationship that needs to be developed that does not exist?			
16.	<i>Do the Social Drivers, Laws, Business Processes, or HIT pose barriers to HIE?</i> Determine if any of the findings for the issue hinder the electronic exchange of health information.			
17.	<i>Should Social Drivers, Laws, Business Processes, or HIT be altered?</i> Determine if it is necessary that the social drivers, business processes, laws, or HIT should be altered to allow for the electronic exchange of health information.			

Alternative Development - Page 2

	Social Drivers	Law	Business Processes	Technical Systems
18.	<i>Analyze Data Social Driver, Law, Business Processes, or HIT Problems.</i> Analyze the information obtained from the research efforts and the above determinations.			
19.	<i>Identify Alternative Solutions:</i> Identify alternative solutions that may resolve the problem. Utilize the alternative criteria provided. Alternatives may be variations of one alternative. There should be more than two alternatives if possible.			
20.	<i>Evaluate Alternative Solutions Against Criteria:</i> Using the criteria provided (process box 3), with another positive or negative affects of the solutions, evaluate each solutions against the criteria. This should result in each potential solution having pros and cons that directly relate to its effectiveness.			
21.	<i>Acquire Feedback:</i> Send the issue analysis as it stands at this point: Issue Statement, Background Information (information gathered from page 1 of the flow process), Alternatives and their Pros and Cons, to stakeholders for input and comments. If appropriate, the issue paper should also be sent to the other Committees for their input. Amend the paper to reflect the feedback as appropriate.			
22.	<i>Determine Alternatives to be Tested:</i> Determine which alternative(s) should be tested. Depending on the availability of a testing			

	environment, only one alternative may be tested. However, if there are two strong alternatives and testing environments exist, two alternatives may be tested simultaneously.
23.	<i>Test by Applying Standards to Scenario or Business Process:</i> Develop criteria against which the effectiveness of the solutions will be tested. Test the alternative utilizing a scenario or a business environment in which the solutions effectiveness can be evaluated.
24.	<i>Alter as Indicated by Testing Results:</i> Determine if there are any problems with the alternative and document the problems. Edit the alternative to the extent necessary.
25.	<i>Retest and Make Required Changes:</i> Retest the alternative: If the alternative fails the second test, determine what caused the failure and re-evaluate the alternatives. Re-determine which alternative should be tested and repeat the process until a solution can be found.
26.	<i>Develop Implementation Specifications:</i> Develop implementation specifications that may be needed to properly implement the recommended solution. These may be determined through the testing process as the solution is implemented into the business environment or tested against the scenario.
27.	<i>Make Final Recommendation:</i> Make a recommendation on the solution for the issue based on the analysis.
28.	<i>Recommend and Publish Final Interoperable Standards:</i> After adopting a viable standard, tool, template, consensus opinion, etc., publish the results.

ENDNOTES

¹ One example scenario from the HISPC project is a patient care scenario: An inpatient specialty substance abuse treatment facility intends to refer client X to a primary care facility for a suspected medical problem. The 2 organizations do not have a previous relationship. The client has a long history of using various drugs and alcohol that is relevant for medical diagnosis. The primary care provider has requested that the substance abuse information be sent by the treatment facility. The primary care provider intends to refer the patient to a specialist and plans to send all of the patient's medical information, including the substance abuse information that was received from the substance abuse treatment facility, to the specialist. Scenario obtained from RTI International's summary "Assessment of Variation and Analysis of Solutions" report to the Office of the National Coordinator for Health IT and Agency for Healthcare Research and Quality, available at <http://www.healthit.ahrq.gov>, accessed June 25, 2007.

² Lisa Rawlins, State of Florida, Testimony before the Health Information Protection Taskforce, February 23, 2007. Also, Jeanne Quarrier, State of New York, Testimony before the Health Information Protection Taskforce, April 26, 2007.

³ The term "consent" is permission, whether written or in electronic form, from individuals to use and disclose their protected health information for purposes defined by law. Under HIPAA, consent is written permission from individuals to use their protected health information for treatment, payment, and health care operations. 45 C.F.R. § 164.506(b). States use the term "consent" interchangeably with the term "authorization." Under HIPAA, however, the term "authorization" is a term of art interpreted differently from "consent." HIPAA defines authorization as written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule. 45 C.F.R. § 164.508. For more information on consent and authorization definitions under HIPAA, see Office for Civil Rights, U.S. Department of Health and Human Services, "Summary of the HIPAA Privacy Rule: HIPAA Compliance Assistance," last revised May 2003, available at <http://www.hhs.gov/ocr/privacysummary.rtf>, accessed on August 9, 2007.

⁴ New York and Minnesota are examples of states that have state law consent requirements for all types of data and for all purposes, even treatment. Alabama and Indiana are examples of states that have no state law consent requirements for health information exchange, whether paper or electronic.

⁵ 45 C.F.R. § 164.506(b).

⁶ RTI International, Interim Assessment of Variation and Analysis of Solutions, December 2006.

⁷ Ibid.

⁸ Ibid.

⁹ Alisa Ray, Certification Commission for Health Information Technology, Testimony before the Health Information Protection Taskforce, April 25, 2007. Also John Loonsk, Director, Office of Interoperability and Standards, Office of the National Coordinator for Health Information Technology, Testimony before the Health Information Communication and Data Exchange Taskforce, July 9, 2007.

¹⁰ Center for Substance Abuse Treatment, Substance Abuse and Mental Health Services Administration, US Department of Health and Human Services, "The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs," June 2004, available at <http://www.hipaa.samhsa.gov/Part2ComparisonCleared.htm>, accessed June 25, 2007.

¹¹ 42 CFR Part 2.

¹² 45 CFR Part section 164.506.

¹³ Ibid. HIPAA uses "may" versus "must" to note flexibility in the implementation of consent components.

¹⁴ §1902(a)(7) of 42 USC §1396a(a)(7) and 42 CFR §431.300 et seq..42 CFR §431.302.

¹⁵ 42 CFR section 431.302.

¹⁶ 42 CFR section 431.305.

¹⁷ 42 CFR section 431.306.

¹⁸ 20 USC 1232g(a)(4).

¹⁹ 45 CFR Part section 164.506.

²⁰ National Association of School Nurses, "Privacy Standards for Student Health Records," Issue Brief, July 2004, available at <http://www.nasn.org/Portals/0/briefs/2004briefprivacy.pdf>.

²¹ The Common Framework Privacy Principles include openness and transparency, purpose specification and minimization, collection limitation, use limitation, individual control and participation, data integrity and quality, security safeguards and controls, accountability and oversight, and remedies. Marcy Wilder, Hogan and Hartson and Steering Committee Member of the Markle Foundation's Connecting for Health, Testimony before the Health Information Protection Taskforce, February 22, 2007. Also Carol Diamond, Markle Foundation, Testimony before the Health Information Protection Taskforce, March 19, 2007. Connecting for Health Common Framework is available at <http://www.connectingforhealth.org/commonframework/>.

²² Personal communication with state representatives, March 2007.

²³ John Lindquist, International Security, Trust, and Privacy Alliance, Testimony before the Health Information Protection Taskforce, April 25, 2007. The updated document reflecting John Lindquist's testimony can be found at "Analysis of Privacy Principles: Making Privacy Operational," version 2.0, May 2007, available at <http://www.istpa.org/index.cfm>.

²⁴ Deven McGraw, National Partnership for Women & Families, Testimony before the Health Information Protection Taskforce, March 19, 2007.

²⁵ Marcy Wilder, February 2007 testimony.

²⁶ Discussed during June 2007 HIP/HISPC meeting. Michigan and Oregon used scenarios to provide the consumers with real-world applications of eHIE. These states found that the more they explained what eHIE is about, the more consumers desired it. In Rhode Island's case, the state initially decided on an opt-out approach to its eHIE, meaning that all consumers in the state would be participants of the exchange unless they opted from participation. After surveying a sample of its population, Rhode Island discovered that the consumers actually preferred to voluntarily participate in the exchange instead of automatically being assumed to be participants of the exchange.

²⁷ Personal communication with Mark Leavitt, Chair of the Certification Commission for Health Information Technology, July 13, 2007.

²⁸ This recommendation had one dissenting vote from a Health Information Protection Taskforce member.

²⁹ Executive Order 13410: Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs, August 22, 2006, available at <http://www.whitehouse.gov/news/releases/2006/08/print/20060822-2.html>, accessed August 9, 2007.