Summary of Policy Recommendations from the Markle Foundation's Connecting for Health Common Framework

Purpose: This document summarizes the policies from various policy documents from the Connecting for Health Common Framework initiative under the auspices of the Markle Foundation. This document was developed to distill a summarized version of Common Framework policies that could be useful in health information exchange development initiatives. This recapitulation covers Common Framework policy principles and policy documents P1 to P8 that can be found at http://www.connectingforhealth.org/commonframework/index.html.

Connecting for Health's Policy Principles[1]

Openness and Transparency
There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.

Purpose Specification and Minimization
The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.

Collection Limitation
Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.

Use Limitation
Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.

Individual Participation and Control
Individuals should control access to their personal information:

- Individuals should be able to obtain from each entity that controls personal health data, information about whether or not the entity has data relating to them.
- Individuals should have the right to:
    - Have personal data relating to them communicated within a reasonable time (at an affordable charge, if any), and in a form that is readily understandable;
    - Be given reasons if a request (as described above) is denied, and to be able to challenge such denial; and
    - Challenge data relating to them and have it rectified, completed, or amended.

[1] The Common Framework: Overview and Principles, Connecting for Health, Markle Foundation, 2006, p. 4.

Data Integrity and Quality
All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.

Security Safeguards and Controls
Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.

Accountability and Oversight
Entities in control of personal health data must be held accountable for implementing these information practices.

Remedies
Legal and financial remedies must exist to address any security breaches or privacy violations.

Connecting for Health's Technology Principles[2]

Make it "Thin"
Only the minimum number of rules and protocols essential to widespread exchange of health information should be specified as part of a Common Framework. It is desirable to leave to the local systems those things best handled locally, while specifying at a national level those things required as universal in order to allow for exchange among subordinate networks.

Avoid "Rip and Replace"
Any proposed model for health information exchange must take into account the current structure of the healthcare system. While some infrastructure may need to evolve, the system should take advantage of what has been deployed today. Similarly, it should build on existing Internet capabilities, using appropriate standards for ensuring secure transfer of information.

Separate Applications from the Network
The purpose of the network is to allow authorized persons to access data as needed. The purpose of applications is to display or otherwise use that data once received. The network should be designed to support any and all useful types of applications, and applications should be designed to take data in from the network in standard formats. This allows new applications to be created and existing ones upgraded without re-designing the network itself.

Decentralization
Data stay where they are. The decentralized approach leaves clinical data in the control of those providers with a direct relationship with the patient, and leaves judgments about who should and should not see patient data in the hands of the patient and the physicians and institutions that are directly involved with his or her care.

Federation
The participating members of a health network must belong to and comply with agreements of a federation. Federation, in this view, is a response to the organizational difficulties presented by

[2] The Common Framework: Overview and Principles, Connecting for Health, Markle Foundation, 2006, p. 5.

the fact of decentralization. Formal federation with clear agreements builds trust that is essential to the exchange of health information.

Flexibility
Any hardware or software can be used for health information exchange as long as it conforms to a Common Framework of essential requirements. The network should
support variation and innovation in response to local needs. The network must be able to scale and evolve over time.

Privacy and Security
All health information exchange, including in support of the delivery of care and the conduct of research and public health reporting, must be conducted in an environment of trust, based upon conformance with appropriate requirements for patient privacy, security, confidentiality, integrity, audit, and informed consent.

Accuracy
Accuracy in identifying both a patient and his or her records with little tolerance for error is an essential element of health information exchange. There must also be feedback mechanisms to help organizations to fix or "clean" their data in the event that errors are discovered.

COMMON FRAMEWORK POLICY GUIDES

Architecture for Privacy in a the Networked Health Information Exchange
Privacy Architectural Principles[3]

1. **Openness and Transparency:** There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.
2. **Purpose Specification and Minimization:** The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.
3. **Collection Limitation:** Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.
4. **Use Limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.
5. **Individual Participation and Control:** Individuals should control access to their personal information; Individuals should be able to obtain from each entity that controls personal health data, information about whether or not the entity has data relating to them. Individuals should have the right to:
   - Have personal data relating to them communicated within a reasonable time (at an affordable charge, if any), and in a form that is readily understandable;
   - Be given reasons if a request (as described above) is denied, and be able to challenge such denial; and
   - Challenge data relating to them and have it rectified, completed, or amended.
6. **Data Integrity and Quality:** All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.

[3] P1 – The Architecture for Privacy in a Networked Health Information Environment, Connecting for Health, Markle Foundation, April 2006. Summary table pp. 1-7.

7. **Security Safeguards and Controls:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.
8. **Accountability and Oversight:** Entities in control of personal health data must be held accountable for implementing these information practices.
9. **Remedies:** Legal and financial remedies must exist to address any security breaches or privacy violations.

Model Privacy Policies and Procedures for Health Information Exchange

Recommended Policy Language[4] included in Model HIE Contract

Policy 100: Compliance with Law and Policy

1. **Laws.** Each Participant shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of individually identifiable health information and establishing certain individual privacy rights. Each Participant shall use reasonable efforts to stay abreast of any changes or updates to and interpretations of such laws and regulations to ensure compliance.
2. **HIE Policies.** Each Participant shall, at all times, comply with all applicable HIE policies and procedures ("HIE Policies"). These HIE Policies may be revised and updated from time to time upon reasonable written notice to Participant. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these HIE Policies.
3. **Participant Policies.** Each Participant is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and these HIE Policies. In the event of a conflict between these HIE Policies and an institution's own policies and procedures, the Participant shall comply with the policy that is more protective of individual privacy and security.

Policy 200: Notice of Privacy Practices

Each Participant shall develop and maintain a notice of privacy practices (the "Notice") that complies with applicable law and this Policy.

1. **Content.** The Notice shall meet the content requirements set forth under the HIPAA Privacy Rule[6] and comply with all applicable laws and regulations. The Notice also shall include a description of the HIE and the RLS and inform individuals regarding: (1) what information the institution may include in and make available through the HIE and the RLS; (2) who is able to access the information in the HIE and the RLS; (3) for what purposes such information can be accessed; and (4) how the individual can have his or her information removed from the RLS.
2. **Provision to Individuals.** Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals, which policies and procedures shall be consistent with this Policy and comply with applicable laws and regulations.
    1. For Participants that are health care providers, the Notice shall be: (1) available to the public upon request; (2) posted on all web sites of the Participant and available electronically through such sites; (3) provided to a patient at the date of first service delivery; (4) available at the institution; and (5) posted in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the Notice.
    2. For Participants that are health plans, the Notice shall be: (1) available to the public upon request; (2) provided to new enrollees at the time of plan enrollment; (3) provided to current plan enrollees within 60 days of a material revision; and (4) posted on the plan's web sites and available electronically through such sites. Participating health plan institutions also shall

[4] P2 – Model Privacy Policies and Procedures for Health Information Exchange, Connecting for Health, Markle Foundation, April 2006 pp. 3-12.

notify individuals covered by the plan of the availability of the Notice and how to obtain a copy at least once every three years.

3. **Individual Acknowledgement.** Each Participant that is a health care provider shall make a good faith effort to obtain the individual's written acknowledgement of receipt of the Notice or to document their efforts and/or failure to do so. The acknowledgement of the Notice shall comply with all applicable laws and regulations. Each Participant shall have its own policies and procedures governing obtaining an acknowledgement, which policies and procedures shall be consistent with this Policy and comply with applicable laws and regulations.
4. **Participant Choice.** Participants may choose a more proactive notice distribution process than provided herein and may include more detail in their notice of privacy practices. Possible additional protections for individuals whose information may be made available through the RLS (not all of which pertain to notice policies alone) could include: mailing the revised notice or a notification letter allowing for removal or exclusion of the information about that individual from the RLS to every individual prior to loading the information into the RLS or shortly thereafter; excluding individuals from the RLS index unless individual consent is obtained; loading individual information into the RLS on a going-forward, new individual encounter basis only; developing a method for time-stamping an RLS record to indicate when the record was loaded into the index; developing a method for allowing individuals to limit access to their RLS records; and obtaining individual consent prior to each inquiry made to the RLS index by a Participant, or on a periodic basis.

Policy 300: Individual Participation and Control of Information Posted to the RLS

1. **Choice Not to Have Information Included in the RLS.** All individuals may choose not to have information about them included in or made available through the RLS.
2. **Effect of Choice.** An individual's choice not to have information about him or her included in or made available through the RLS shall be exercised through the Participant, as described in the institution's Notice, after which time the institution shall no longer include the individual in the RLS. Participants shall develop and implement appropriate mechanisms to remove information about an individual from the RLS if the individual chooses to have such information excluded from the RLS.
3. **Revocation.** An individual who has chosen not to make information concerning him or her available through the RLS subsequently may be included in the RLS only if the individual revokes his or her decision or subsequently chooses to renew participation in the RLS.
4. **Documentation.** Each Participant shall document and maintain documentation of all patients' decisions not to have information about them included in the RLS.
5. **Participant Choice.** Participants shall establish reasonable and appropriate processes to enable the exercise of a patient's choice not to have information about him or her included in the RLS. Each Participant retains the authority to decide whether and when to obtain patient consent prior to making information available through the RLS.
6. **Provision of Coverage or Care.** A Participant shall not withhold coverage care from an individual on the basis of individual's choice not to have information about him or her included in the RLS.

Policy 400: Uses and Disclosures of Health Information

1. **Compliance with Law.** All disclosures of health information through the HIE and the use of information obtained from the HIE shall be consistent with all applicable federal, state, and local laws and regulations and shall not be used for any unlawful discriminatory purpose. If applicable law requires that certain documentation exist or that other conditions be met prior to using or disclosing health information for a particular purpose, the requesting institution shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of such at the request of the disclosing institution.
2. **Purposes.** A Participant may request health information through the RLS or HIE only for purposes permitted by applicable law. Each Participant shall provide or request health

information through the RLS or HIE only to the extent necessary and only for those purposes that are permitted by applicable federal, state, and local laws and regulations and these Policies. Information may not be requested for marketing or marketing related purposes without specific patient authorization. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a permissible purpose, a Participant may not request information through the RLS or from the HIE.

3. **HIE Policies.** Uses and disclosures of and requests for health information via the HIE shall comply with all HIE Policies, including, but not limited to, the HIE Policy on Minimum Necessary and the HIE Policy on Information Subject to Special Protection.
4. **Participant Policies.** Each Participant shall refer to and comply with its own internal policies and procedures regarding disclosures of health information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making such disclosures.
5. **Accounting of Disclosures.** Each Participant disclosing health information through the HIE shall work towards implementing a system to document the purposes for which such disclosures are made, as provided by the requesting institution, and any other information that may be necessary for compliance with the HIPAA Privacy Rule's accounting of disclosures requirement.[24] Each Participant is responsible for ensuring its compliance with such requirement and may choose to provide individuals with more information in the accounting than is required. Each requesting institution shall provide information required for the disclosing institution to meet its obligations under the HIPAA Privacy Rule's accounting of disclosures requirement.
6. **Audit Logs.** Participants and HIEs shall consider and work towards maintaining an audit log documenting which Participants posted and accessed the information about an individual through the RLS and when such information was posted and accessed.[25] Participants and HIEs shall consider and work towards implementing a system wherein, upon request, patients have a means of seeing who has posted and who has accessed information about them through the RLS and when such information was accessed.
7. **Authentication.** Each Participant shall follow uniform minimum authentication requirements for verifying and authenticating those within their institutions who shall have access to, as well as other Participants who request access to, information through the HIE and/or the RLS.
8. **Access.** Each HIE should have a formal process through which information in the RLS can be requested by a patient or on a patient's behalf.[29] Participants and HIEs shall consider and work towards providing patients direct access to the information contained in the RLS that is about them.

Policy 500: Information Subject to Special Protection

Some health information may be subject to special protection under federal, state, and/or local laws and regulations (e.g., substance abuse, mental health, and HIV). Each Participant shall determine and identify what information is subject to special protection under applicable law prior to disclosing any information through the HIE. Each Participant is responsible for complying with such laws and regulations.

Policy 600: Minimum Necessary

1. **Uses.** Each Participant shall use only the minimum amount of health information obtained through the HIE as is necessary for the purpose of such use. Each Participant shall share health information obtained through the HIE with and allow access to such information by only those
1. workforce members, agents, and contractors who need the information in connection with their job function or duties.
2. **Disclosures.** Each Participant shall disclose through the HIE only the minimum amount of health information as is necessary for the purpose of the disclosure. Disclosures to a health care provider for treatment purposes and disclosures required by law are not subject to this Minimum Necessary Policy.
3. **Requests.** Each Participant shall request only the minimum amount of health information through the HIE as is necessary for the intended purpose of the request. This Minimum Necessary Policy does not apply to requests by health care providers for treatment purposes.

4. **Entire Medical Record.** A Participant shall not use, disclose, or request an individual's entire medical record except where specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request. This limit does not apply to disclosures to or requests by a health care provider for treatment purposes or disclosures required by law.

Policy 700: Workforce, Agents, and Contractors

1. **Access to System.** Each Participant shall allow access to the HIE only by those workforce members, agents, and contractors who have a legitimate and appropriate need to use the HIE and/or release or obtain information through the HIE. No workforce member, agent, or contractor shall be provided with access to the HIE without first having been trained on these Policies, as set forth below.
2. **Training.** Each Participant shall develop and implement a training program for its workforce members, agents, and contractors who will have access to the HIE to ensure compliance with these Policies. The training shall include a detailed review of applicable Policies and each trained workforce member, agent, and contractor shall sign a representation that he or she received, read, and understands these Policies.
3. **Discipline for Non-Compliance.** Each Participant shall implement procedures to discipline and hold workforce members, agents, and contractors accountable for ensuring that they do not use, disclose, or request health information except as permitted by these Policies and that they comply with these Policies. Such discipline measures shall include, but not be limited to, verbal and written warnings, demotion, and termination and provide for retraining where appropriate.
4. **Reporting of Non-Compliance.** Each Participant shall have a mechanism for, and shall encourage, all workforce members, agents, and contractors to report any noncompliance with these Policies to the Participant. Each Participant also shall establish a process for individuals whose health information is included in the RLS to report any non-compliance with these Policies or concerns about improper disclosures of information about them.

Policy 800: Amendment of Data

Each Participant shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information. If an individual requests, and the Participant accepts, an amendment to the health information about the individual, the Participant shall make reasonable efforts to inform other Participants that accessed or received such information through the HIE, within a reasonable time, if the recipient institution may have relied or could foreseeably rely on the information to the detriment of the individual.

Policy 900: Requests for Restrictions

If a Participant agrees to an individual's request for restrictions, as permitted under the HIPAA Privacy Rule, such Participant shall ensure that it complies with the restrictions when releasing information through the HIE. If an agreed-upon restriction will or could affect the requesting institution's uses and/or disclosures of health information, at the time of disclosure, the Participant disclosing such health information shall notify the requesting institution of the fact that certain information has been restricted, without disclosing the content of any such restriction.

Policy 1000: Mitigation

Each Participant shall implement a process to mitigate, and shall mitigate and take appropriate remedial action, to the extent practicable, any harmful effect that is known to the institution of a use or disclosure of health information through the HIE in violation of applicable laws and/or regulations and/or these Policies by the institution, or its workforce members, agents, and contractors. Steps to mitigate could include, among other things, Participant notification to the individual of the disclosure of information about them or Participant request to the party who received such information to return and/or destroy the impermissibly disclosed information.

Notification and Consent When Using a Record Locator Service

Selected statements[5]: The HIPAA Privacy Rule would permit participation in the RLS system without a provision requiring for notice to the patient or patient authorization. The Privacy Rule permits covered entities to "use or disclose protected health information for treatment, payment, or health care operations" without first obtaining an individual's authorization for such use or disclosure. Treatment is defined as "the provision, coordination, or management of health care and related services by one or more health care providers."[4] Health care operations is broadly defined and includes, for example: "[c]onducting quality assessment and improvement activities, including outcomes evaluation…[and] population-based activities relating to improving health or reducing health care costs."[5] The information sharing that the RLS is designed to facilitate falls squarely within the HIPAA sanctioned uses and disclosures that do not require patient authorization. Therefore, the following proposed notice and patient choice policies go above and beyond what is required by the federal HIPAA privacy law and further than what a number of local and regional interoperable systems, such as the Indiana Network for Patient Care, currently require.

Recommendations[6] (Policy):

1. Patients should be given notice that their health care provider or health plan participates in a system that provides an electronic means for locating their medical records across the providers they are seeing (the RLS). Individuals should also be provided with an opportunity to choose not to have such information about them included in the system. Moreover, the Policy Subcommittee recommends that patients should retain the ability to choose not to participate in the RLS system at any time. It is noted again that these policy recommendations apply only to patient information contained in the RLS; the decision as to whether or not to release clinical records in a given circumstance remains with the individual institution or provider holding the records, acting in compliance with its own disclosure policies, the stated desires of patients, when relevant, and applicable federal and state laws.
2. The operational burden created by requiring that notice be given to patients prior to an institution's initial loading of patient information into the RLS index might not be practical in some settings and might threaten the robustness and viability of the two-step approach designed to separate actual clinical data from information about the location of that data in order to limit risk of exposure while at the same time enabling early and significant value in health information exchange. Therefore information regarding patients of a participating institution generally be included in the RLS index on day one and going forward. The index would include only patient names, non-clinical details used to identify the patient (name, date of birth, etc.), and participating institutions where that patient has had care. The index would not include patient clinical records. The question of whether information regarding patients previously seen at the participating institution should be posted to the index, and the details of that information (age of information, etc.), would be left to the participating institution.
3. Participating institutions and providers are encouraged to exercise additional means of providing for notice and patient choice with regard to participation in the RLS as they deem feasible and appropriate. For example, institutions could choose to provide for written notice and the opportunity to choose not to participate in the RLS to patients prior to an institution's initial loading of patient information into the RLS index, either en masse, or on an individual basis during patient encounters. An institution or provider might also choose to contact patients via electronic means for those patients for whom it has such information. Finally, the design of the RLS relies in the first instance on the participating institution or provider to decide whether to load patient information into the RLS at all.

[5] P3 – Notification and Consent When Using a Record Locator Service, Connecting for Health, Markle Foundation, April 2006 pp. 2-3.

[6] P3 – Notification and Consent When Using a Record Locator Service, Connecting for Health, Markle Foundation, April 2006 pp. 3-4-

4. **Notice of Privacy Practices.** In accordance with these recommendations, Participants must revise their HIPAA Notice of Privacy Practices to include provisions describing the RLS and to offer an opportunity for individuals to choose not to be included in the RLS. The description must include: (1) what information is included in and made available through the RLS; (2) who is able to access information in the RLS; (3) for what purposes such information can be accessed; and (4) how the patient can choose not to have his or her information from that institution included in the RLS. All patients must be given the HIPAA Privacy Notice during their initial encounter with a provider. Many institutions provide notice at every service delivery date. In addition, the notice must be available at the institution and on request, posted "in a clear and prominent location where it is reasonable to expect individuals seeking service…to be able to read the notice," and posted on the institution's web site.
5. **Initial Inquiry Audit.** Individual participants and HIEs should consider and work towards implementing a system that enables an "initial inquiry audit." In such a system, individual participants and HIEs would work towards developing a method so that the first time an inquiry is made to the RLS index regarding a particular patient, the patient would be given notice explaining that information about them is included in a system that provides an electronic means for locating their medical records across providers they are seeing (the RLS) and explaining how the patient may choose to have that information excluded from the RLS in the future.
6. **Patient Access to RLS Record.** Participants and HIEs should consider and work towards implementing a system wherein, upon request, patients are provided direct access to the information contained in the RLS that is about them.
7. Since current options for direct patient access and authentication to the RLS are not robust enough to be implemented without the possibility of introducing serious vulnerability to the security of the system, each HIE should have a formal process through which information in the RLS can be requested by a patient or on a patient's behalf.

Correctly Matching Patients with Their Records

Selected statements[7]: Health institutions with large numbers of records must rely on probability to declare that a given record or set of records matches a set of identifiers (name, gender, date of birth, etc.). The risk of this strategy, of course, is that the matches so recorded may not be accurate. There is some risk of "false negatives"—records that pertain to a patient but are not found. There is a much greater risk, however, from "false positives"—matches with records that do not pertain to the subject patient, but are wrongly returned in a search. False positive matches carry two forms of risk—privacy risk and clinical risk. The privacy risk is that records pertaining to patients not under the care of a particular clinician will be delivered, exposing personal details to those who have no need for them. The clinical risk is that a clinician will make a decision based on information that is erroneous because it is actually information about a different person, not the subject patient. Although clinicians are trained to make allowances for the fact that there is a significant error rate in clinical information when they make important decisions, the technology for handling such matches still needs to be optimized for a high degree of certainty, and where incorrect matching does occur, the system should err on the side of returning false negatives rather than false positives.

The RLS must implement a matching algorithm for queries using a sometimes incomplete subset of the possible constellation of demographic details. Authorized queriers present a set of demographic details and receive in return zero or more matching record locations. Probability weighted matching can improve the quality of record matching by taking the specific characteristics of records in particular databases into account.

[7] P4 – Correctly Matching Patients with Their Records, Connecting for Health, Markle Foundation, April 2006 pp. 1-2

Recommendations[8] (Policy):

1. It is assumed that an RLS false positive match is an incidental disclosure pursuant to HIPAA, with the understanding that such a disclosure is permissible under the law only to the extent that the covered entity or entities involved have applied reasonable safeguards and implemented the minimum necessary standard.
2. There should be a minimum level of certainty before the RLS returns information to the requester; and that whenever that level of certainty is not reached, the RLS could request additional demographic fields until either the level of certainty is reached or no record can be returned. These levels could be set in order to minimize to the extent possible incidental disclosures of protected health information in an effort to respect the privacy of patients for ethical and public policy reasons.
3. In the case in which a requester of information recognizes that information received from the RLS does not apply to the patient about whom information was requested, the requester should take reasonable steps to immediately destroy that information, including, where applicable, deleting the electronic version of that portion of the RLS response and/or any paper copies thereof.

Authentication of System Users

Definitions[9]:

Identity: Identity is, in this context, an individual person or institution that needs access to health care data, for any purpose. Crucially, an identity is not merely a role; if you want to know the identity of someone who authorized a particular prescription, you want to know that it was Dr. Smith, not just that it was a doctor.

Identifier: An identifier is an attribute that points unambiguously and uniquely to an identity. In practice, the person identifier will often be an employee ID number, or, possibly, a log-in name guaranteed unique within the scope of the institution. It is critical that such identifiers not be re-issued to other, later users. If "jsmith" is used as an identifier, all future John or Jane Smiths must be issued a different identifier. (Note that this policy will require a tightening of existing policy for those institutions that currently allow for re-use of identifiers.) An identifier is an abstract attribute and generated attribute of a particular person or entity, in the case of institutional identifiers. Tokens that refer to roles such as "Primary Care Physician," or those referring to institutional relations such as "Admitting Privileges at General Hospital" are not considered identifiers in this context. The problem is often expressed in terms of issuing identities, which means, in practice, issuing unique identifiers that correspond uniquely and unambiguously to an existing identity, in the manner of providing an employee ID or unique login.

Authentication: Authentication requires an identifier, and is required for authorization. Authentication is a way of allowing a user to prove that he is who he claims to be. The simplest form of authentication is in the providing of an identifying token, plus a secret of some sort, such as a bank card + PIN, or a username + password or phrase. An example of how not to handle authentication is the SSN. One of the reasons the SSN has turned out to be a bad identifier is that one number is meant to provide the function of both the public and secret parts of authentication: you have an SSN that points uniquely to you, but you must reveal it as proof that you have it. Without being accompanied by a second, secret token such as a PIN, the SSN is damaged in regard to authentication by the very use that makes it otherwise worthwhile.

Authorization: After a user claiming a given identity has been authenticated, an authorization mechanism needs to determine what data the user is allowed to access and what functions may be performed by the user on that data, e.g., to view, copy, or update data. Authorization is typically role-based; that is, the different operations available are tied to the role of the user, such as physician,

[8] P4 – Correctly Matching Patients with Their Records, Connecting for Health, Markle Foundation, April 2006 pp. 3-5.

[9] P5 – authentication of System Users, Connecting for Health, Markle Foundation, April 2006 pp. 2-3.

administrative support, etc. One individual can have many roles within the system (for example, Primary Care Physician, Admitting Physician, Specialist, etc.).
Break the Glass: In the event of a health care emergency, some method may be provided to allow access in the event of an authentication failure as a kind of "Break the Glass" function on an existing account. However, role-based authorization is not sufficient for use of the system; no access to the system should be allowed for any such role without a human identifier attached. It is not enough to ask that someone prove that they have admitting privileges at General Hospital; they must also provide their actual identity, so that should a later audit be required, a person can be associated with the audited actions, not just a role.

Requirements[10] (Policies):
Every transaction involving patient data between institutions in a HIE will operate by transitive trust, often based in the legal requirements of a contract. The institutional members of a HIE trust one another, and therefore they trust requests from the authenticated and authorized employees of those institutions. The backbone of the transitive trust model is the ability to identify anyone violating that trust, and to link them unambiguously to the entity that gave them access.

Transitive trust is a practical rather than ideal system. Though there has been work on more elaborate federated identity systems, none are yet at a level of practicality necessary for this work, nor are they simple enough to be implemented broadly. The advantages of transitive trust are thus largely practical: it allows systems to scale upwards in the number of employees covered without forcing each institution to know about every other employee in every remote institution. The design and implementation of even a simple system of transitive trust is complex, and will be highly dependent on existing technological tools and frameworks, but all such systems should have the following basic policy restrictions:

- A HIE must have identifiers for all its participating institutions. These identifiers can be issued by the HIE, or they can be adopted from an external source (e.g. HIPAA mandated identifiers[4]), as long as that source guarantees the uniqueness and persistence of any given identifier.
- All users must be authenticated before they are given access to any HIE-wide resource containing patient data. This may take a number of different forms: the local institutions can ask users to log in, and communicate the authenticated identifiers to other participants in the HIE, or the HIE can run authentication services itself, getting lists of users and roles from the participating institutions. This latter strategy may suffer from scaling problems, but may be useful for getting a HIE off the ground.
- Any request for data from a remote institution, an institution other than the one the user is logged in to, must be accompanied by at least two pieces of identifying information: which institution authenticated the requesting user and an identifier for that user. There are a number of ways such a system could be implemented technically, but the basic policy prescription is that, for any given request from a remote institution, the local institution should know where the request came from, and who authorized it.
- A method may be provided to allow access to patient data in the event of an authorization failure—a so-called “Break the Glass” function. Access failure for someone who should be authorized can happen for a number of reasons: he or she does not remember or have the required information or tokens for authentication; or he or she does not have permission from the system to look at or interact with the data they are requesting. Any request that allows a known user to request data they believe they need, e.g., a physician attempting to access the medication history of a patient, when the system would not otherwise give that person access, should be accompanied by a brief description of the rationale for the request.
- No matter what the cause of the authorization failure in the Break the Glass scenario, any system access must be accompanied by an identifier for that user. In no case is an otherwise unidentified “Emergency” account to be used, on the grounds that it amounts to the provisioning of a role without an accompanying person identifier.

[10] P5 – authentication of System Users, Connecting for Health, Markle Foundation, April 2006 pp. 3-4.

- Any request that allows a known user to request data they believe they need, when the system would not otherwise give them access, must be accompanied by enhanced auditing and timely human review.
- The Record Locator Service itself may not offer a Break the Glass function; all such requests must go to the institutions hosting the clinical data.
- In the case of a HIE providing a method for a patient or patient representative to access his or her own records, some "bootstrapping" will be required. The initial issuing of the patient access capability must be done by a participating institution, or by a third-party recognized by the HIE. The patient can then be given a HIE-specific identifier, accompanied by an authentication method, with authorization limited to looking at his or her own material. Depending on implementation within the HIE, the patient could then access his or her records directly after having been issued such credentials, subject to local terms and conditions, and to periodic review. HIE-wide patient access requests, however handled otherwise, must carry the name of the institution that initially created the patient's identifier.

Patients' Access to Their Own Health Information

Selected statements[11]: As a matter of principle, patients should be able to access the RLS. At this stage, however, there are serious privacy and policy issues that must be addressed regarding such access. … Since the RLS may not be covered under the HIPAA Privacy Rule as a provider, plan, or clearinghouse, there may be no legal obligation to provide patients access to the information in the index. But, as a matter of principle, the RLS should be designed to provide such access in a secure, authenticated manner.

Recommendations[12] (Policy):

- Each HIE should have a formal process through which information in the RLS can be requested by a patient or on a patient's behalf.
- Participating entities and HIEs shall consider and work towards providing patients direct, secure access to the information about them contained in the RLS.

Selected (Conclusion) statements[13]: The access provisions of the Privacy Rule serve as an important baseline for ensuring that patients have adequate control over their personal health information. Meanwhile the principles articulated in the **Connecting for Health** "Architecture for Privacy in a Networked Health Information Environment" recommend taking these rights further, establishing that patients should have access to all their information, including information held outside of a covered entity. With this in mind, a discussion about how to give patients access to the information held in the RLS is appropriate. The RLS could ultimately empower patients. Patients' ability to access a reliable list of where their personal health information is stored could significantly enhance their ability to access and potentially amend information.

Auditing Health Information Exchange Access and Use

[11] P6 – Patients' Access to Their Own Health Information, Connecting for Health, Markle Foundation, April 2006 p. 7.
[12] P6 – Patients' Access to Their Own Health Information, Connecting for Health, Markle Foundation, April 2006 p. 8.
[13] P6 – Patients' Access to Their Own Health Information, Connecting for Health, Markle Foundation, April 2006 pp. 8-9.

Recommendations[14] (Policy):

- Recommended audit and accountability checklist that that applies to the HIE and the RLS, and it represents good practice for a broader range of covered entities.
- Audit and Accountability. Audit is the practice of recording the occurrence of selected system events; management uses reports/alerts generated from audit records to monitor the appropriateness of activities. Accountability results when activities are attributable to individuals.
- Logging and audit control functions at the HIE and RLS level should include:
  1. Audit of VIP records.
  2. Procedures for follow-up on suspicious activity, such as indications of possible privacy or security breaches.
  3. Review of network intrusion detection system activity logs.
  4. Review of system administrator authorizations and activity.
  5. Review of physical access to data centers.
  6. Other review of technical, physical, and administrative safeguards as established by the policies of the organization.
- The HIE and the RLS have random audits of demographic and clinical records, based on the level of risk for that portion of the system. The HIE may wish to provide for some level of random audits (sampling) of the participants in the HIE. Random audits should be done for records held at the HIE level and within the RLS. For the RLS and HIE, an independent third-party should perform such random audits, with public reporting of at least the principal results

Breaches of Confidential Health Information

Proposed Policy for HIEs[15]:

A. Compliance with HIPAA Security Rule: The HIE will comply with the HIPAA Security Rule. The HIE Participants will be required to comply with all applicable federal, state, and local laws.

B. Responsibility of Participants to Train Personnel and Enforce Policy: A HIE Participant that may have access to patient data via the HIE network, must appropriately train its personnel and inform them that any breach of confidentiality is actionable. Each Participant should follow and enforce its own institution's confidentiality policies and disciplinary procedures.

C. Notification of Breach: The HIE itself must report **any** breaches and/or security incidents to the particular data provider whose data was improperly used, as in most cases the HIE is a business associate of some or all of its Participants. Each HIE Participant must agree to inform the HIE of any **serious** breach of confidentiality, but is not required to notify the HIE of minor breaches. Participants must also comply with all applicable federal, state, and local laws, which may include laws relating to notification of patients. Participants and HIEs should also work towards implementing a system that ensures affected patients are notified in the event of a breach.

D. Withdrawal from the HIE: Provisions could be included in HIE agreements relating to withdrawal from the HIE. The **Connecting for Health** "Model Contract for Health Information Exchange" provides a variety of model provisions that could allow Participants to terminate their participation freely at any time, require that termination be preceded by a substantial period of advance notice, or require that Participants maintain their participation for a certain period of time. The **Connecting for Health** "Model Contract for Health Information Exchange" also provides a model provision allowing for a Participant to withdraw from a HIE if a serious breach of its patient data has occurred.[5]

[14] P7 – Auditing Access to and Use of a Health Information exchange, Connecting for Health, Markle Foundation, April 2006 pp. 3-5.

[15] P8 – Breaches of Confidential Health Information, Connecting for Health, Markle Foundation, April 2006 pp. 1-2.

HIEs and Participants are encouraged to consider the particular circumstances of small provider practices in developing relevant terms for withdrawal from HIE provisions in their HIE agreements.

E. Indemnification for Breaches of Confidentiality: The **Connecting for Health** "Model Contract for Health Information Exchange" provides a variety of model provisions concerning indemnification. A HIE may also choose to adopt special rules governing indemnification for particular situations, such as a breach of confidentiality of protected health information.