Governance Framework for Trusted Electronic Health Information Exchange

Introduction and Scope

Enabling electronic health information exchange (HIE) requires consensus among multiple stakeholders. Often, complex technical and policy choices are required and, ultimately, governance is established to provide oversight and to hold accountable the parties responsible for exchanging electronic health information. The Governance Framework for Trusted Electronic Health Information Exchange (the Governance Framework) is intended to serve as the Office of the National Coordinator for Health Information Technology's (ONC's) guiding principles on HIE governance. It is meant to provide a common conceptual foundation applicable to all types of governance models and expresses the principles ONC believes are most important for HIE governance. The Governance Framework does not prescribe specific solutions but lays out milestones and outcomes that ONC expects for and from HIE governance entities as they enable electronic HIE.

The Governance Framework's intended audience includes any entities that set HIE policy (e.g., State governments, public-private partnerships, health information exchange organizations (HIOs), private companies) and, in general, is *not* meant to speak directly to "users" of the exchange services governed by such entities). We also believe that third party assessors (e.g., certifying and accrediting organizations) may find the Governance Framework's guiding principles informative as they develop methods to assess the competency, credibility, and trustworthiness of such HIE governance entities.

The Governance Framework reflects ONC's current thinking as well as recommendations of the HIT Policy Committee and HIT Standards Committee. The Governance Framework also draws from ONC's expertise authoring the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information[1] and administering various initiatives to promote electronic health information exchange at local and national levels. ONC expects to update and adapt the Governance Framework over time to reflect stakeholder feedback, policy changes, technological maturity, and market innovations.[2]

Organizational Principles

The entity that sets HIE policy plays a central role in the success of an electronic HIE initiative. It has a primary responsibility to instill confidence among governed organizations, their users (e.g., health care providers and patients), and other exchange partners regarding the way in which electronic exchange is conducted. With respect to the way in which an entity that sets HIE policy performs its duties[3], we believe that it should:

1. Operate with transparency and openness.
2. Establish mechanisms to ensure that the entity's policies and practices and applicable federal and state laws and regulations are adhered to.

---

[1] http://www.healthit.gov/policy-researchers-implementers/nationwide-privacy-and-security-framework-electronic-exchange

[2] Entities that set HIE policy must comply with all applicable existing legal requirements. The Governance Framework's principles were drafted to comply with legal requirements in effect at the time they were drafted and do not preempt any existing or future statutory and regulatory requirements that conflict with them.

[3] See HIT Policy Committee Recommendation #1 transmitted to the National Coordinator in December 2010. http://www.healthit.gov/sites/default/files/hitpc_transmittal_letter_gov_wg_dec2010.pdf

3. Promote inclusive participation and adequate stakeholder representation (especially among patients and patient advocates) in the development of policies and practices.
4. Ensure its oversight is consistent and equitable.
5. Provide due process to the stakeholders to which it provides oversight.

Trust Principles

Trust is a prerequisite for electronic HIE and starts with patients. Without trust, the ultimate success of an electronic HIE initiative could be jeopardized. With respect to the trust, we believe an entity that sets HIE policy is responsible for creating an environment in which patients should:

1. Be able to publicly access, in lay person terms, a "Notice of Data Practices.[4]" Such notice would explain the purpose(s) for which personally identifiable and de-identified[5] data, consistent with applicable laws, would or could be electronically exchanged (e.g., treatment, payment, research, quality improvement, public health reporting, population health management).
2. Receive a simple explanation of the privacy and security policies and practices that are in place to protect their personally identifiable information when it is electronically exchanged and who is permitted to access and use electronic HIE services.
3. Consistent with applicable laws, be provided with meaningful choice as to whether their personally identifiable information can be electronically exchanged.[6]
4. Consistent with applicable laws, be able to request data exchange limits based on data type or source (e.g., substance abuse treatment).
5. Consistent with applicable laws, be able to electronically access and request corrections to their personally identifiable information.
6. Be assured that their personally identifiable information is consistently and accurately matched when electronically exchanged.

Business Principles

Successful electronic HIE requires cooperation among all parties. Responsible financial and operational HIE policy is vital to improving care coordination, improving the efficiency of health care delivery, and mitigating behaviors that could result in proprietary networks and resistance to exchanging information even when it could enhance patient care. With respect to how an entity that sets HIE policy ensures electronic exchange occurs with the patient's best interests in mind, we believe that it should:

1. Set standards of participation that promote collaboration and avoid instances where (even when permitted by law) differences in fees, policies, services, or contracts would prevent patients' health information from being electronically exchanged.
2. Provide open access to exchange services (e.g., directory data) that would enable local, regional, and nationwide partners to identify who they can electronically exchange information with and how such exchange could be completed under applicable laws and regulations.

---

[4] Note that the "Notice of Data Practices" would be different than the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Notice of Privacy Practices of the participating covered entities.

[5] The term "de-identified" is intended to have the same meaning as it does in the HIPAA Privacy Rule at 45 CFR 164.514.

[6] This principle expresses ONC's general belief as informed by the HITPC recommendations dated September 1, 2010. We recognize that further policy may be necessary to develop more specific guidance related to the various electronic exchange scenarios in which meaningful choice may or may not be deemed appropriate.

3. Publish statistics describing their electronic exchange capacity, including, for example: number of users, the types of standards implemented, number of patient lives covered, and transaction volume.
4. Maintain and disseminate up-to-date information about: compliance with relevant statutory and regulatory requirements; available standards; potential security vulnerabilities, and best practices developed for HIE.

Technical Principles

Electronic HIE requires technical conformance at multiple levels and the consistent implementation of highly specified and rigorously tested implementation specifications. With respect to the expectations of technical conformance and use of standards an entity that sets HIE policy promotes, we believe that it should:

1. Ensure that technology is implemented to support the Trust and Business Principles.
2. Prioritize, where available, the exclusive use of federal vocabulary, content, transport, and security standards and associated implementation specifications adopted to support HIE.[7]
3. Encourage the use of vocabulary, content, transport, and security standards, and associated implementation specifications developed by voluntary consensus standards organizations (VCSOs) when equivalent federal standards have not been adopted.
4. Lead engagement in VCSOs and national efforts to accelerate standards development and consensus on the adoption of standards as well as the improvement of existing standards.
5. Work with VCSOs to develop standards for specific use cases and volunteer to pilot and use new standards when no such standards exist.
6. Take an active role in development and implementation of conformance assessment and testing methods for HIE and utilize (or promote the use of) testing methods developed to assess compliance with federal standards.

To find out more about ONC's overall approach to HIE governance and to follow our continued efforts related to this initiative please visit our website at http://www.healthit.gov/HIEgovernance.

[7] Such standards include, but are not limited to those adopted by ONC [http://www.healthit.gov/policy-researchers-implementers/meaningful-use-stage-2-0/standards-hub; various Federal Information Processing (FIPS) Standards and Special Publications authored by NIST [http://csrc.nist.gov/publications/PubsFIPS.html & http://csrc.nist.gov/publications/PubsSPs.html]; and the standards and implementation specifications of the HIPAA Privacy and Security Rules, and the HITECH Breach Notification Rule (45 CFR 164 Parts 160 & 164 subparts C, E, & F) which are administered by the HHS Office for Civil Rights [http://www.hhs.gov/ocr/privacy]