NHIN POLICY AND TECHNOLOGY FRAMEWORK - DRAFT 6/10/2010

POLICY PRINCIPLES

1. Individual Access
2. Correction
3. Openness and Transparency
4. Individual choice
5. Collection, Use and Disclosure Limitation
6. Data Integrity and Quality
7. Safeguards
8. Accountability

TECHNOLOGY PRINCIPLES

1. Keep it simple
2. Keep the implementation cost as low as possible
3. Don't let "perfect" be the enemy of "good enough"
4. Design for the little guy
5. Do not try to create a one-size-fits-all standard
6. Separate content and transmission standards.
7. Create publicly available vocabularies & code sets
8. Leverage the web for transport ("health internet").
9. Position quality measures so they motivate standards adoption.
10. Support implementers

Principle (from ONC Nationwide Principles)	Policy Expectations	Policy Practice Requirements	Technology Requirements	Enforcement[1] (Accountability and Oversight)	Comments
Individual Access – (*P1 Architecture for Privacy* - http://www.connectingforhealth.org/commonframework/docs/T1_TechIssues.pdf) individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format	• Providers/record holders should provide individuals with prompt electronic access to, and copies of, their health information, at a reasonable cost	• Prohibitions on unauthorized use • Breach notification policies (*P8: Breaches of Confidential Information* - http://www.connectingforhealth.org/commonframework/docs/P8_Breaches.pdf) • Anti-discrimination and compelled disclosures (*CP2: Policy Notice to Consumers* - http://www.connectingforhealth.org/phti/docs/CP2.pdf) • Proxy access • Ability to terminate account on line • Patient access to their own Records (P6)	• Identification and authentication requirements for individuals (*P5: Authentication of System Users* - http://www.connectingforhealth.org/commonframework/docs/P5_Authentication_SysUsers.pdf and *CT2: Authentication of Users* - http://www.connectingforhealth.org/phti/reports/ct2.html) • Secure access, storage (*CT6* - http://www.connectingforhealth.org/phti/reports/ct6.html) • Download capability • Secure data import and export (*CT5* - http://www.connectingforhealth.org/phti/reports/ct5.html, CT, *CT6* - http://www.connectingforhealth.org/phti/reports/ct6.html) • Immutable audit trail (*CT3* - http://www.connectingforhealth.org/phti/reports/ct3.html) • Limitations on indentifying information	• Burden is on record holders to comply • New HIPAA access rules • Meaningful use criteria	Which kinds of entities will be allowed to provision consumers with NHIN-Direct accounts? There may be many different ways for consumer to gain access to PHI -- Keeping policies in synch is key.

[1] Final ONC Principle on Accountability is the foundation for this column: **Accountability** – These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

Principle (from ONC Nationwide Principles)	Policy Expectations	Policy Practice Requirements	Technology Requirements	Enforcement[1] (Account-ability and Oversight)	Comments
			• (*CT4* - http://www.connectingforhealth.org/phti/reports/ct4.html)		
Correction – Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.	• Providers/record holders should establish process for resolving disputes about the content of the record (HHS to develop and disseminate model processes?) • Providers/record holders should educate patients and their family members about the process. • Providers must either make corrections to the record or append explanation if requested by patient (HIPAA)	• Clear mechanisms to resolve complaints identified (*CP6 Dispute Resolution* - http://www.connectingforhealth.org/phti/docs/CP6.pdf) • Opportunity to correct erroneous information and an obligation to correct or delete information that is erroneous; • (*CP6 Dispute Resolution* - http://www.connectingforhealth.org/phti/docs/CP6.pdf)	• Technology for ensuring patient-amended information is subsequently sent in that format • Do we require push notification of changes to previously distributed information? (this would be difficult!) • Special requirements for preventing edits to "forwarded" information – such as digital signature? • How is "amended" information officially communicated back to the provider's record?	• HIPAA rules re: requesting a correction to the record	

Principle (from ONC Nationwide Principles)	Policy Expectations	Policy Practice Requirements	Technology Requirements	Enforcement[1] (Accountability and Oversight)	Comments
	• Providers must take reasonable steps to notify any recipients of incorrect information (see tech. question about push notification) • Information that is "amended" by a patient may only be subsequently accessed, used or disclosed with the amendment				
Openness and Transparency – there should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information	• Providers/record holders will need to educate their patients about the transformation to electronic records and what it means for how their information is accessed, used and disclosed (HHS to develop / disseminate model notification provisions; suggestions for improving patient understanding?)	• Notices should be easily accessible, clear, comprehensive, summarized, updated. • (*CP2 Policy Notice to Consumers* - http://www.connectingforhealth.org/phti/docs/CP2.pdf) • Policies regarding acceptable uses and disclosures of individual health care information, ensuring individual participation in and control of their health information (P2 Model Privacy Policies and Procedures)		• HIPAA notice already required – better guidance/ models from OCR/ONC?	

Principle (from ONC Nationwide Principles)	Policy Expectations	Policy Practice Requirements	Technology Requirements	Enforcement[1] (Accountability and Oversight)	Comments
Individual Choice (Individual Participation and Control) – Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information.	• Providers/record holders are responsible for complying with any existing federal or state consent requirements – (*P1 Architecture for Privacy* - http://www.connectingforhealth.org/commonframework/docs/T1_TechIssues.pdf) • Providers/record holders should be clear to patients and their families when consent or authorization is needed	• A complete framework of protections • Specific, "independent consent" is important for practices that would be unexpected by a reasonable consumer • (*CP2 Policy Notice to Consumers* - http://www.connectingforhealth.org/phti/docs/CP2.pdf)	• Indication that any required consent has been obtained? • Data segmentation/flags for information covered by special consent rules?	• Enforcement of federal/state laws?	Accountable Care Orgs (ACO) will create new demands for analytics on individuals and populations, leveraging comprehensive HIE data. Standardize on opt-in versus opt-out?

Principle (from ONC Nationwide Principles)	Policy Expectations	Policy Practice Requirements	Technology Requirements	Enforcement[1] (Accountability and Oversight)	Comments
Collection, use and disclosure limitation– (*P1 Architecture for Privacy* - http://www.connectingforhealth.org/commonframework/docs/T1_TechIssues.pdf) - individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplished a specified lawful purpose(s) and never to discriminate inappropriately	• Providers/data holders should collect, use and disclose only the minimum necessary amount of information to accomplish the lawful, intended purpose • Access to and use of data by users and by intermediaries access should be clearly specified be limited to the very specific scope that has been specified with safeguards to limit unnecessary disclosures or access	• **Purpose specification:** The purposes for which personal data are collected should be specified • **Collection limitation and data minimization**: Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. • **Use limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified. • **Disclosure limitation:** For machines or intermediaries that manage the lookup or routing of records over the network, there should be no exposure of personally identifiable health information (including metadata, data types, or content)	• Data segmentation/flags? • Technologies that mask identifying information? • Technical specifications and standards for information sharing should limit any disclosure of personally identifiable data or metadata that exposes an individual's clinical or health information on the network or to intermediaries or machines involved in the exchange. • (*T2 HIE Implementation Guide* - http://www.connectingforhealth.org/commonframework/docs/T2_HealthInfo.pdf)	• Burden is on data holders to make this determination prior to access, use or disclosure (per HITECH) • HIPAA minimum necessary rules (do not apply to treatment disclosures) • Commitments made in agreements with data "trading partners"?	HIEs will want to sell "services" based on aggregated data – how will this be managed?

Principle (from ONC Nationwide Principles)	Policy Expectations	Policy Practice Requirements	Technology Requirements	Enforcement[1] (Accountability and Oversight)	Comments
Data quality and integrity – (*T5 Background Issues on Quality* - http://www.connectingforhealth.org/commonframework/docs/T5_Background_Issues_Data.pdf) persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.	• Providers/data holders should establish an internal process for ensuring health data is complete and accurate (?) • Providers/data holders are responsible for disclosing accurate representation of what is in their records	• Common redress strategies: Notice of a possible adverse decision using inaccurate data and the procedure for challenging it; • Ability to trace information to its source for verification; • Procedures for ensuring that erroneous information does not re-enter the system; • Correctly matching patients with their records	• Automatic notification in the event of data conflicts? • Tools for quality control, as well as regular backups and redundancy in systems and databases. • Produce and make available audit logs (*P7 Auditing Access* - http://www.connectingforhealth.org/commonframework/docs/P7_Auditing_Access.pdf)	• Commitment made in agreement(s) with data "trading partners" • Independent administrative or judicial review and enforcement.	

Principle (from ONC Nationwide Principles)	Policy Expectations	Policy Practice Requirements	Technology Requirements	Enforcement[1] (Accountability and Oversight)	Comments
Safeguards – individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use or disclosure	• Providers/data holders should establish reasonable policies and processes for ensuring internal accountability for health information • Providers/data holders should disclose electronic health information only to legitimate persons/entities (provider with treatment relationship, public health authority, etc.) • Providers/data holders should send copies of individual's data only to the subject or other authorized individual • Intermediaries (HISPs) facilitating transport or performing identification and authentication of providers or individuals should have access only to data that is necessary to accomplish the purpose (no to limited PHI in message, limited to no access to PHI in payload)	• Physical Security and Access Security policies (*P5: Authentication of System Users* - http://www.connectingforhealth.org/commonframework/docs/P5_Authentication_SysUsers.pdf) • Breach notification policies • MORE HERE	• Identification and authorization of providers (*P5: Authentication of System Users* - http://www.connectingforhealth.org/commonframework/docs/P5_Authentication_SysUsers.pdf) • Identification and authorization of individuals • Technologies used for transport should support limited access to data by intermediaries/HISP (*T2 HIE Implementation Guide* - http://www.connectingforhealth.org/commonframework/docs/T2_HealthInfo.pdf) • Establish tools for user authentication and access (*P5: Authentication of System Users* - http://www.connectingforhealth.org/commonframework/docs/P5_Authentication_SysUsers.pdf)	• Meaningful use/certification criteria? • Commitments made in agreements among data "trading partners"? • Limitations on intermediary access to data is enforced by business associate rules/BA agreements and accreditation?	Technology standards for distributed consent management are immature and complex, expensive to implement.

Principle (from ONC Nationwide Principles)	Policy Expectations	Policy Practice Requirements	Technology Requirements	Enforcement[1] (Accountability and Oversight)	Comments
			• Promote technological choices that limit the potential for abuse and mitigate risks of large breaches, including distributed architecture where appropriate (*T2 HIE Implementation Guide* - http://www.connectingforhealth.org/commonframework/docs/T2_HealthInfo.pdf) • HISP to HISP transmissions should use encrypted channel (in addition to payload encryption.)		
Remedies	• Establish mechanisms for complaints • Establish remedies for affected parties to compensate for harm caused by breach				

Additional Principles from Strategic Framework White Paper	Policy Expectations	Policy Practice Requirements	Technology Requirements	Enforcement (Accountability and Oversight)
Policies and technical specifications required and/or promoted by the Federal government should, at a minimum, allow providers to achieve meaningful use of HIT			• Specific NHIN Direct policies/specs should focus only on what is needed for MU	
The federal government should leverage market innovation in information and communications technologies to foster appropriate health information exchange				
Effective health information exchange should enable all participants in the exchange, including patients, to contribute toward achieving meaningful use				I foresee increased tension around PHRs as trusted sources of information for providers to use. PHR versus HIE versus "Health Bank" – new models may be needed.
Policies and technical specifications should be kept as simple as possible and be designed for implementation by all participants.			• NHIN Direct specs should leverage the Internet and be easy to use across a broad spectrum of providers.	
Policies and technical specifications should be patient-centered and make possible and promote increased patient engagement and access (part of individual access principle above?)				

Additional Principles from Strategic Framework White Paper	Policy Expectations	Policy Practice Requirements	Technology Requirements	Enforcement (Accountability and Oversight)
Privacy and Security Solutions should enhance privacy and security while facilitating the appropriate access, use and exchange of health information to achieve health outcomes				
Privacy and Security Solutions should be flexible to adapt to evolving technical capabilities over time				

Markle Connecting for Health Resources: (see separate doc.)