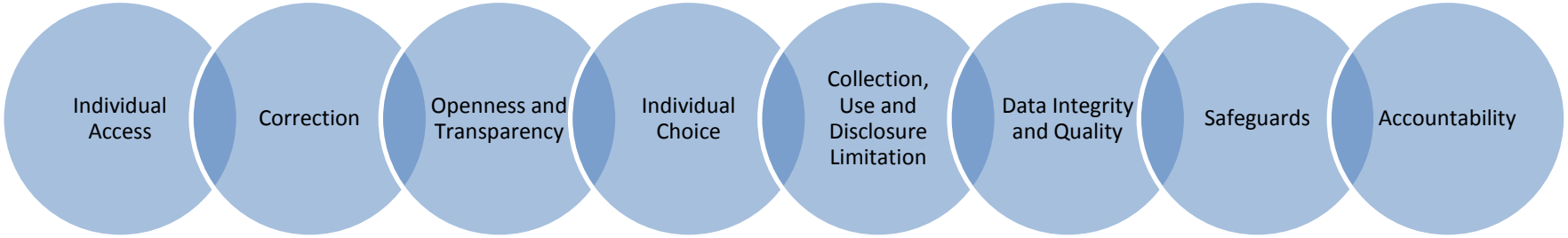
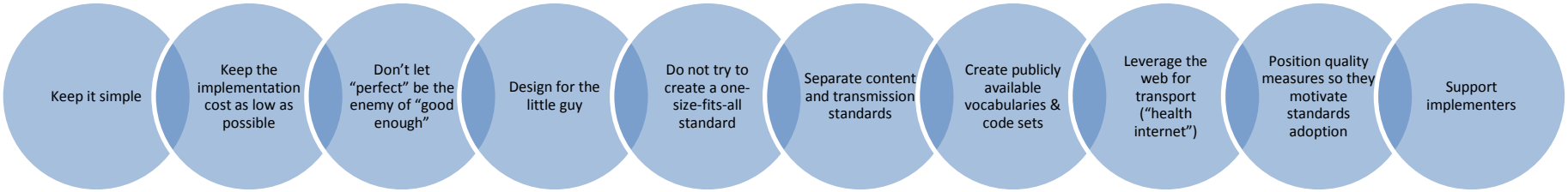
POLICY AND TECHNOLOGY FRAMEWORK FOR HEALTH INFORMATION EXCHANGE



Policy Principles	
Individual Access	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. (P1 Architecture for Privacy)
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.
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.
Individual choice	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.
Collection, Use and Disclosure Limitation	Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified lawful purpose(s) and never to discriminate inappropriately. (P1 Architecture for Privacy)
Data Integrity and Quality	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. (T5 Background Issues on Quality)
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.
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.

POLICY AND TECHNOLOGY FRAMEWORK FOR HEALTH INFORMATION EXCHANGE



Technology Principles	
Keep it Simple	Think big but start small. Recommend standards as minimal as required to support a necessary policy objective or business need, and then build as you go.
Keep the implementation cost as low as possible	Minimize the costs associated with implementation of standards, including royalties, licensing fees and other expenses. Open the NIST interoperability certification testing processes.
Don't let "perfect" be the enemy of "good enough	Go for the 80 percent that everyone can agree on. Get everyone to send the basics (meds, problems, allergies, labs) before focusing on the more obscure.
Design for the little guy	Make sure the endorsed standards are as broadly implementable as possible, so diverse participants can adopt it, and not only the best resourced.
Do not try to create a one-size-fits-all standard	Do not mandate or attempt to create a one-size-fits-all standard that adds burden or complexity to the simple use cases.
Separate content and transmission standards	Separate content standards from transmission standards; ie., if CCD is the html, what is the https? Separate the network layer from the application layer. Avoid linking changes between senders and receivers.
Create publicly available vocabularies & code sets	Ensure they are easily accessible and downloadable, with straightforward means to update or upgrade.
Leverage the web for transport ("health internet"	Use what already works in transporting information securely on the internet. Decrease complexity as much as possible to shorten the learning curve of implementers.
Position quality measures so they motivate standards adoption	Strive for quality reporting to be an automated by-product of using certified technology and standards, lowering the administrative burden of reporting to the lowest extent possible.
Support implementers	Make Implementation Guides available that are human readable, with working examples and testing tools. Facilitate implementers' use of Implementation Guides with effective national communication plans. Publish open source reference implementations.

Individual Access

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.

	Policy	Technology Implications **Certification Criteria for EHR Technology Final Rule**	Accountability and Oversight (Enforcement Levers)
Current Law/Regulation	An individual's right of access generally applies to the information that exists within a covered entity's designated record set(s). Covered entities must (1) respond to requests for access in a timely manner; (2) develop and implement reasonable policies and procedures to verify the identity and authority of any person who requests PHI; (3) provide access to the PHI in the form or format requested by the individual, if it is readily producible, and (4) provide denials--as permitted under the Privacy Rule-- in a timely manner, in writing, and in plain language. Individuals have the right to receive an accounting of certain disclosures. Per HITECH Act, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information of an individual, that individual shall have a right to obtain from the covered entity a copy of information in an electronic format.	*Access control*. Assign a unique name and/or number for identifying and tracking user identity, establish controls that permit only authorized users to access information. *Emergency access*. Permit authorized users to access electronic health information during an emergency. *Authentication*. Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information. *Electronic copy of health information*. Enable a user to create an electronic copy of a patient's clinical information. *Timely access*. Enable a user to provide patients with online access to their clinical information.	
Tiger Team Recommendations	*Topic TBD*		
Notes/Considerations	• Anti-discrimination and compelled disclosures (CP2: Policy Notice to Consumers) • 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 and CT2 Authentication of Users) • Secure access, storage (CT6) • Download capability • Secure data import and export (CT5, CT, CT6) • Immutable audit trail (CT3) • Limitations on indentifying information (CT4)	• Burden is on record holders to comply • New HIPAA access rules • Meaningful use criteria

POLICY AND TECHNOLOGY FRAMEWORK FOR HEALTH INFORMATION EXCHANGE

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.			
	Policy	**Technology Implications** **Certification Criteria for EHR Technology Final Rule**	**Accountability and Oversight (Enforcement Levers)**
Current Law/Regulation	Individuals have the right to have a covered entity amend their PHI in a designated record set; covered entity must act timely, usually within 60 days, to amend the record as requested by the individual or to notify the individual the request is denied; covered entity must make reasonable efforts to see that the amended information is provided generally to persons identified by the individual as having received the info. and who need to know about the amendment and others who covered entity has reason to believe would rely on information, including its business associates.		
Tiger Team Recommendations	Topic TBD		
Notes/Considerations	• Clear mechanisms to resolve complaints about accuracy or completeness of health information identified CP6 Dispute Resolution) • Opportunity to correct (vs. amend?) erroneous information and an obligation to correct or delete information that is erroneous;(CP6 Dispute Resolution) • Who has obligation to amend if error occurs downstream (need to check impact of HITECH)	• Technology for ensuring patient-amended information is subsequently sent in that format • Do we require push notification of changes to previously distributed information? Required by rule to a certain extent. • Special requirements for preventing edits to "forwarded" information – such as digital signature? • How is "amended" information officially communicated back to the provider's record? • Generally, provider who created the information is responsible for amending.	HIPAA rules re: requesting a correction to the record

POLICY AND TECHNOLOGY FRAMEWORK FOR HEALTH INFORMATION EXCHANGE

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.			
	Policy	**Technology Implications** **Certification Criteria for EHR Technology Final Rule**	**Accountability and Oversight (Enforcement Levers)**
Current Law/Regulation	Requires that providers provide individuals with a Notice of Privacy Practices (NPP); attempt to obtain written acknowledgement; post the NPP on its website; provide an electronic copy of the NPP when the first health care service is provided electronically; and may email the NPP to an individual if the individual agrees. Notice required specifies uses and disclosures permitted by HIPAA PR without the individual's written authorization, not actual privacy practices of the covered entity.	Disclosures. Record disclosures made for treatment, payment, and health care operations.(Certification criterion made optional)	

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.

	Policy	Technology Implications Certification Criteria for EHR Technology Final Rule	Accountability and Oversight (Enforcement Levers)
Tiger Team Recommendations	• Third party service organizations should be obligated to disclose in their business associate or service agreements with their customers how they use and disclose information, including without limitation their use and disclosure of de-identified data, their retention policies and procedures, and their data security practices.(Rec. 1) • Requesting providers who are not covered by HIPAA should disclose this to the disclosing provider before patient information is exchanged. (Rec. 2.2) • Providers are responsible for being open and transparent with their patients about how their data is exchanged; providers also should be encouraged to discuss information exchange practices with patients, particularly where there is a new significant development such as "indirect exchange" through a business associate that triggers consent per our previous recommendations • Providers should provide the Notice of Privacy Practices (NPP) as a layered notice - a short summary of information sharing policies and activities should be required for all patients. This "summary notice" should indicate how to obtain more information; a more detailed notice for interested patients should also be readily available; the notice should not only be in plain English but should be written at a reading level that most of a covered entity's patients would understand and presented in compliance with applicable laws with respect to language and disability. The notice should ideally cover current and anticipated exchange activities in lieu of merely describing what the law permits. • All patients should receive a brief summary description of the indirect exchange model, including the name(s) of the organization(s) with legal responsibility for managing the indirect exchange model and the purposes for which information can be shared by or through the model. Notice of the provider's intent to participate in "indirect exchange" should take place before the patient's record leaves the control of the provider. Patients must have an ability to obtain more detailed written information about the indirect exchange model, such as the names/identities of other participants. Providers may provide this directly to patients or rely upon the exchange to provide the information • All patients should receive summary information about the provider's participation in OHCAs and that generally describes how other entities that are part of or share records with the OHCA will have access to the patient's information. As with the notice required for participation in an indirect sharing arrangement, it should be distinct and not be buried in the HIPAA notice. Patients should have an ability to obtain more detailed written information; including a list of the other entities in the OHCA that have access to their information. The provider may provide this information to patients directly or refer the patient to easy-to-find organizational resources. • ONC should require federally funded HIOs and Regional Extension Centers to develop and implement public education plans regarding their information sharing policies and practices. ***Source:*** *Privacy & Security Tiger Team Recommendation on Transparency [PDF - 42 KB]*		

POLICY AND TECHNOLOGY FRAMEWORK FOR HEALTH INFORMATION EXCHANGE

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.			
	Policy	**Technology Implications** **Certification Criteria for EHR Technology Final Rule**	**Accountability and Oversight (Enforcement Levers)**
Notes/Considerations	• Notices should be easily accessible, clear, comprehensive, summarized, updated. (CP2 Policy Notice to Consumers) • 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?

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.

	Policy	Technology Implications Certification Criteria for EHR Technology Final Rule	Accountability and Oversight (Enforcement Levers)
Current Law/Regulation	Provides an individual with the right to (1) agree or object to, or authorize, certain disclosures and (2) request restrictions of certain uses and disclosures. Permits a covered entity to obtain consent for certain uses and disclosures.		
Tiger Team Recommendations	• Directed exchange for treatment does not require patient consent beyond what is required in current law or what has been customary practice. (Rec. 3.1) • When the decision to disclose or exchange the patient's identifiable health information from the provider's record is not in the control of the provider or that provider's organized health care arrangement (OHCA), patients should be able to exercise *meaningful consent* to their participation. ONC should promote this policy through all of its levers. (Note: Applies to stage 1 MU.)(Rec. 3.2 & 3.3) • The person who has the direct, treating relationship with the individual—usually a provider—holds the trust relationship and is responsible for educating and discussing with patients about how information is shared and with whom. (Rec. 3.4) • The provider/provider entity is responsible for obtaining and keeping track of patient consent, but may delegate this function to a third party. (Rec. 3.4) • Providers have choice with respect to participation in HIE. (Rec. 3.5) • The technology for supporting granular patient consent is promising but is still in the early stages of development. ONC should explore this further and in the meantime, patients should be educated about the extent to which their requests can be honored. (Rec.4) • The exchange of identifiable health information for "treatment" should be limited to treatment of the individual who is the subject of the information, unless the provider has the consent of the subject individual. (Rec. 5)		
Notes/Considerations	• 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) • 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?	• Indication that any required consent has been obtained? • Data segmentation/flags for information covered by special consent rules?	Enforcement of federal/state laws?

Collection, use and disclosure limitation Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified lawful purpose(s) and never to discriminate inappropriately.			
	Policy	**Technology Implications** **Certification Criteria for EHR Technology Final Rule**	**Accountability and Oversight (Enforcement Levers)**
Current Law/Regulation	Requires covered entities and business associates to limit uses, disclosures, and requests of protected PHI to the minimum necessary; and defines and limits the uses and disclosures covered entities may make without an individual's authorization; implement reasonable policies and procedures to limit the information disclosed or requested.	*Digest.* Create a message digest. *Data Integrity.* Verify upon receipt of electronically exchanged health information that such information has not been altered. *Detection.* Detect the alteration of audit logs. *Submission.* Enable a user to electronically submit calculated clinical quality measures. *Public health surveillance.* Electronically record, modify, retrieve,and submit syndrome-based public health surveillance information.	
Tiger Team Recommendations	• Third party service organizations may not collect, use or disclose personally identifiable health information for any purpose other than to provide the services specified in the business associate or service agreement with the data provider, and necessary administrative functions, or as required by law. (Rec. 1) • Third party service organizations may retain personally identifiable health information only for as long as reasonably necessary to perform the functions specified in the business associate or service agreement with the data provider, and necessary administrative functions. (Rec. 1) • Public health and quality reporting by providers (or HIOs acting on their behalf) should take place using the least amount of identifiable data necessary to fulfill the lawful public health purpose for which the information is being sought. (Rec. 5) • The exchange of identifiable health information for "treatment" should be limited to treatment of the individual who is the subject of the information, unless the provider has the consent of the subject individual. (Rec. 5)		• When third party service organizations have access to PHI, they must execute and be bound by business associate agreements under HIPAA. Further work is needed on governance issues. Rec. 1) • The responsibility for maintaining the privacy and security of a patient's record rests with the patient's providers, who may delegate functions as long as such delegation maintains this trust. (Rec. 2.1) • Providers who exchange personally identifiable health information should comply with applicable state and federal privacy and security rules. If a provider is not a HIPAA-covered entity or business associate, other mechanisms to secure enforcement and accountability should be used. (Rec. 2.2)

Collection, use and disclosure limitation Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified lawful purpose(s) and never to discriminate inappropriately.			
	Policy	**Technology Implications** **Certification Criteria for EHR Technology Final Rule**	**Accountability and Oversight (Enforcement Levers)**
Notes/Considerations	• **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) • HIEs will want to sell "services" based on aggregated data – how will this be managed?	• 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)	• 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"?

Data quality and integrity 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			
	Policy	**Technology Implications** **Certification Criteria for EHR Technology Final Rule**	**Accountability and Oversight (Enforcement Levers)**
Current Law/Regulation	The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI; specifically, covered entities must ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; identify and protect against reasonably anticipated threats to the security or integrity of the information; protect against reasonably anticipated, impermissible uses or disclosures; and ensure compliance by their workforce.	*Record actions*. Record actions related to electronic health information. *Generate audit log*. Enable a user to generate an audit log for a specific time period and to sort entries in the audit.	
Tiger Team Recommendations	Five categories of recommendations for patient matching: • Standardized formats for demographic data fields • Internally evaluating matching accuracy, including individual providers and institutions as well as HIEs in the evaluations, make use of performance improvement metrics • Accountability, implement and enforce governance policies and levels of accuracy model • Developing, promoting and disseminating best practices for improving data capture and matching accuracy, ensure transparency re: the efficacy of matching algorithms • Supporting the role of the individual/patient in identifying errors in their health and demographic information; simplifying processes for redress and correction • EHRs should be tested and certified for interoperability; consider using a USPS validation/normalization program to improved matching accuracy; support the efforts of the Meaningful Use Workgroup and the Policy Committee to increase the access of individuals to their health information ***Source:*** *Privacy & Security Tiger Team Recommendation on Patient Matching*		
Notes/Considerations	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)	• Commitment made in agreement(s) with data "trading partners" • Independent administrative or judicial review and enforcement.

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.			
	Policy	**Technology Implications** **Certification Criteria for EHR Technology Final Rule**	**Accountability and Oversight (Enforcement Levers)**
Current Law/Regulation	Requires covered entities to implement appropriate administrative, technical, and physical safeguards to protect the PHI; establishes protections for PHI in all forms: paper, electronic, and oral; safeguards include such actions and practices as securing locations and equipment; implementing technical solutions to mitigate risks; and workforce training. Meaningful use: Conduct security risk assessment required by Privacy Rule	*General encryption*. Encrypt and decrypt electronic health information. *Automatic log-off*. Terminate an electronic session after a predetermined time of inactivity.	

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.			
	Policy	**Technology Implications** **Certification Criteria for EHR Technology Final Rule**	**Accountability and Oversight (Enforcement Levers)**
Tiger Team Recommendations	• Tiger Team recommendations on consent for directed exchange assume the information exchanged is sent securely. • The requesting provider in an exchange should, at a minimum, provide attestation of his or her treatment relationship with the individual who is subject of the health information exchange. (Rec. 2.2) • Providers should be required for meaningful use to have a plan for how they will utilize certified EHR technology security functionality • Require a high level of assurance that the organization is who it says it is; all entities involved in health data exchange should be required to have digital certificates; requirements for digital certificates should include organization verification, validation transactions meet MU, reliance on existing criteria and processes when applicable; PHI transactions should require authenticated digital certificates • Process for issuing digital certificates and process for re-evaluation, e.g., annual renewal • ONC should establish an accreditation program for reviewing and authorizing certificate issuers, and select or specify standards for digital certificates • With respect to individual users, provider entities and organizations must develop and implement policies to identity proof and authenticate their individual users (already required under HIPAA Security Rule) ***Source:*** *Privacy & Security Tiger Team Recommendations on Provider Authentication* ***Note:*** *User and patient authentication (including identity proofing and authentication) recommendations will be presented to the HIT Policy Committee on 04-13-2011*		

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.			
	Policy	**Technology Implications** **Certification Criteria for EHR Technology Final Rule**	**Accountability and Oversight (Enforcement Levers)**
Notes/Considerations	• Physical Security and Access Security policies (P5: Authentication of System Users) • Breach notification policies • Technology standards for distributed consent management are immature and complex, expensive to implement..	• Identification and authorization of providers (P5: Authentication of System Users) • Identification and authorization of individuals • Technologies used for transport should support limited access to data by intermediaries/HISP (T2 HIE Implementation Guide) • Establish tools for user authentication and access (P5: Authentication of System Users) • Promote technological choices that limit the potential for abuse and mitigate risks of large breaches, including distributed architecture where appropriate (T2 HIE Implementation Guide) • HISP to HISP transmissions should use encrypted channel (in addition to payload encryption.)	• 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?