DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Office of the National Coordinator
for Health Information Technology
Washington, D.C. 20201

Program Information Notice

Document Number: ONC-HIE-PIN-003

Date: March 22, 2012

Document Title: Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program

To: State Health Information Exchange Cooperative Agreement Program Award Recipients

As stated in the State Health Information Exchange Cooperative Agreement Program Funding Opportunity Announcement (FOA), the Office of the National Coordinator for Health Information Technology (ONC) may offer program guidance to provide assistance and direction to states and State Designated Entities (SDEs) that receive awards under the program. This Program Information Notice (PIN) provides additional direction to states and SDEs receiving funding under the State Health Information Exchange Cooperative Agreement Program on privacy and security frameworks required as part of grantee strategic and operational plan (SOP) updates.

The National Quality Strategy sets three aims for improving health care in our country: better care, affordable care, and healthy people and communities. Information that is accurate, up to date, and available when and where a patient seeks care is the lifeblood of health care improvement and crucial to reaching these goals. The stage is set for the nation to make rapid progress on health information exchange (HIE) this year supporting achievement of the three-part aim.

This PIN guidance provides a common set of privacy and security rules of the road to assure provider and public trust and enable rapid progress in health information exchange to support patient care. It addresses concerns from State leaders and other stakeholders that health information exchange efforts have been hampered and slowed by the lack of consistent approaches to core privacy and security issues and responds to requests for clear national guidance.

The guidance in this PIN builds from the privacy and security and governance recommendations of the Health IT Policy Committee as well as the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*[1].

[1] http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173

This PIN guidance will be used by State Health Information Exchange Cooperative Agreement recipients to establish robust privacy and security policies and practices for health information exchange services as outlined in the Funding Opportunity Announcement (FOA) and in the first PIN issued by the State HIE Program.

But the guidance will also be of great utility to state policy leaders and other stakeholders working diligently to establish common privacy and security policies and practices for communities, regions and states to enable provider and public trust and support rapid progress in health information exchange. This PIN can serve as a framework and offer specific direction and guidance to these efforts.

If you have any questions or require further assistance, please contact your Project Officer.

Sincerely,

Farzad Mostashari

National Coordinator for Health Information Technology

PURPOSE

This PIN provides direction to states and SDEs receiving funding under the State Health Information Exchange Cooperative Agreement Program on approaches to ensuring private and secure health information exchange of individually identifiable health information (IIHI) and on requirements for privacy and security frameworks submitted as part of 2012 annual updates to grantee SOPs.

APPLICABILITY

This guidance is applicable to all ONC State Health Information Exchange Cooperative Agreement Program recipients (hereafter referred to as "recipients"), whether the recipient is a state government or a state designated entity (SDE).

Please note that the terms "shall" and "should" are used in very specific ways in this document. "Shall" represents a mandatory action while "should" reflects a recommended course of action within the State HIE Program.

The requirements and guidance discussed in this PIN are not intended to and do not supercede any applicable provisions of Federal or State law, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations.

REQUIREMENTS FOR SUBMISSION

As part of their 2012 annual SOP updates, recipients shall submit their privacy and security frameworks consisting of all relevant statewide policies and practices adopted by recipients, and any operational policies and practices for health information exchange services being implemented by the recipient or funded in whole or in part with federal cooperative agreement funds. Please refer to Appendix A to determine which domains and specific guidance are applicable to the specific HIE architectural approach the recipient is taking and must be addressed. Recipients may use the template in Appendix A as a guide and tool for completing the privacy and security framework for 2012 SOP updates.

DISCUSSION

Recipients shall use this PIN guidance to do the following:

- Determine which domains and relevant guidance need to be addressed based on the architectural approach the recipient is taking (see Appendix A).
- Review existing privacy and security policies and practices to identify where the recipient's approach aligns with the specific guidance provided for each domain (see "State Health Information Exchange Cooperative Agreement Program Guidance on Privacy and Security Frameworks"), and where gaps exist.
- Where privacy and security policies and practices align with the specific guidance provided for each domain, include these policies and practices as part of the 2012 annual SOP update.
- Where there are gaps in recipient privacy and security policies and practices, i.e., a domain is not addressed or policies are not in alignment with the specific guidance

provided for each domain, include a strategy, timeline and action plan for addressing these gaps in the 2012 SOP update.

Policies and practices may apply to HIE operations or to organizations and providers participating in exchange. Where recipients are funding multiple local health information organizations (HIOs) or other exchange efforts, Project Officers will provide guidance to cooperative agreement recipients on details to include in 2012 SOP updates.

State Health Information Exchange Cooperative Agreement Program Guidance on Privacy and Security Frameworks

This guidance addresses the core domains of the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*[2], built from the fair information practice principles (FIPPs) that have guided privacy and security efforts worldwide for decades:

1. Individual access
2. Correction
3. Openness and transparency
4. Individual choice
5. Collection, use and disclosure limitation
6. Data quality and integrity
7. Safeguards
8. Accountability

State HIE Cooperative Agreement Program recipients should use the following guidance to evaluate their current privacy and security policies and practices and determine if alignment gaps exist. State policy makers and other stakeholders can use the guidance to determine, assess and fill gaps in current policies and practices to assure trusted health information exchange. The guidance outlines a core set of privacy and security expectations that should be consistently applied, but it is not exhaustive. Recipients will have additional policies and requirements that are critical to their efforts.

Please refer to Appendix A to determine which domains should apply, depending on the services provided and the architecture being used.

Domains: Individual Access and Correction

Individual Access. Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information (IIHI) in a readable form and format.

Correction. Individuals should be provided with a timely means to dispute the accuracy or integrity of their IIHI, and to have erroneous information corrected or to have a dispute documented if their requests are denied.

Specific Guidance

Where HIE entities store, assemble or aggregate IIHI, such as longitudinal patient records with data from multiple providers, HIE entities should make concrete plans to give patients electronic access to their compiled IIHI and develop clearly defined processes (1) for individuals to request

[2] http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173

corrections to their IIHI and (2) to resolve disputes about information accuracy and document when requests are denied.

Domain: Openness and Transparency

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.

Specific Guidance

Individuals should be able to determine what information exists about them, how it is collected, used or disclosed and whether they can exercise choice over any of these elements. Where HIE entities store, assemble or aggregate IIHI, individuals should have the ability to request and review documentation to determine who has accessed their information or to whom it has been disclosed. All policies and procedures consistent with the recipient's Privacy and Security Framework should be communicated to individuals in a manner that is appropriate and understandable.

HIE policies should make publicly available a notice of data practices describing why IIHI is collected, how it is used, and to whom and for what reason(s) it is disclosed. This notice should be:

1. Simple, understandable, and at an appropriate literacy level.

2. Highlight, through layering or other techniques the disclosures and uses that are most relevant (for example, the notice of privacy practice could have a summary sheet followed by a description of actual use and disclosure practices).

3. Adhere to obligations for use of appropriate language(s) and accessibility to people with disabilities.

HIE policies should also encourage health care providers to be open and transparent with patients about their privacy and security practices and to discuss HIE with their patients.

Domain: Individual Choice

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. Individuals should be able to designate someone (family member, caregiver, domestic partner or legal guardian) to make decisions on their behalf. This process should be fair and not burdensome.

Specific Guidance

Where HIE entities serve solely as information conduits for directed exchange of IIHI and do not access IIHI or use IIHI beyond what is required to encrypt and route it, patient choice is not

required beyond existing law. Such sharing of IIHI from one health care provider directly to another is currently within patient expectations.

Where HIE entities store, assemble or aggregate IIHI beyond what is required for an initial directed transaction, HIE entities should ensure individuals have meaningful choice regarding whether their IIHI may be exchanged through the HIE entity. This type of exchange will likely occur in a query/response model or where information is aggregated for analytics or reporting purposes.

A patient's *meaningful choice* means that choice is:

1. Made with advance knowledge/time;
2. Not used for discriminatory purposes or as condition for receiving medical treatment;
3. Made with full transparency and education;
4. Commensurate with circumstances for why IIHI is exchanged;
5. Consistent with patient expectations; and
6. Revocable at any time.

Both opt-in and opt-out models can be acceptable means of obtaining patient choice provided that choice is meaningful (i.e., use of either model must meet the requirements described above and not be limited to, for example, a provider's boilerplate form or reliance on the patient to read material posted on a provider's waiting room wall or website).

Where meaningful choice is required, HIE entities should either (1) directly ensure patients have the opportunity for meaningful choice; or (2) ensure that the health care providers for which it facilitates electronic health information exchange provide individuals with meaningful choice regarding the exchange of their IIHI. Choice should be offered to each patient on a prospective basis and periodically renewed.

Attention should be paid to minimizing provider burden.

Individuals should have choice about which providers can access their information. In addition, recipients are encouraged to develop policies and technical approaches that offer individuals more granular choice than having all or none of their information exchanged.

Domain: Collection, Use and Disclosure Limitation

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 purpose and never to discriminate inappropriately. This information should only be collected, used or disclosed to accomplish a specific purpose, and purposes of information exchange should be specified.

Specific Guidance

Providers requesting or accessing IIHI by electronic means for "treatment" should have or be in the process of establishing a treatment relationship with the patient who is the subject of the requested information. The means of verifying whether such a relationship exists could include attestation or artifacts such as patient registration, prescriptions, consults, and referrals.

In principle, a health care provider should only access the minimum amount of information needed for treatment of the patient.

This guidance does not apply to de-identified data and would not otherwise apply to public health authorities that are legally authorized to receive the requested information. Neither does the guidance apply to situations where the patient has clearly and specifically given permission to the provider to access his/her information for treatment of another patient. For example, a woman could give permission for her health information to be accessed by a health care provider for treatment of her sister.

Domain: Data Quality and Integrity

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.

Specific Guidance

Where HIE entities store, assemble or aggregate IIHI, they should implement strategies and approaches to ensure the data exchanged are complete and accurate and that patients are correctly matched with their data. Processes should also be developed and documented to detect, prevent, and mitigate any unauthorized changes to, or deletions of, individually identifiable health information.

HIE entities that store, assemble or aggregate IIHI should also develop processes to communicate corrections in a timely manner to others with whom this information has been shared.

Recipients should describe their patient matching approach including the accuracy threshold achieved.

Domain: Safeguards

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.

Specific Guidance

HIE entities should conduct a thorough assessment of risks and vulnerabilities. Please refer to the State HIE Security Checklist at: http://hitrc-collaborative.org/confluence/display/hiecopprivacyandsecurity/Security. This checklist may serve as a resource to assist HIE entities in evaluating their compliance with the HIPAA Security Rule and the Breach Notification Rule. Use of this checklist does not guarantee compliance; however, because safeguards must be evaluated within the specific context in which information is assembled, held and transmitted. It may be useful to retain a completed version of the checklist for record keeping.

Encryption. HIE entities should provide for the exchange of already encrypted IIHI, encrypt IIHI before exchanging it, and/or establish and make available encrypted channels through which electronic health information exchange could take place.

Authentication and Authorization. An HIE entity should only facilitate electronic health information exchange for parties it has authenticated and authorized. Verification of identity, authentication of users, and authorization of individuals could be accomplished directly by the HIE or indirectly by providers or other entities.

HIE entities should establish strong identity proofing and authentication policies for user access to electronic health information systems. Recipients should indicate the assurance level they are using in their privacy and security frameworks, using NIST 800-63 version 1.0.2[3] as a guide and resource. The recommended assurance level is Level 3.

Domain: Accountability

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.

Specific Guidance

HIE entities should ensure appropriate monitoring mechanisms are in place to report and mitigate non-adherence to policies and breaches. Reasonable mitigation strategies should be established and implemented as appropriate, including notice to individuals of privacy violations and security breaches.

---

[3] *csrc.**nist**.gov/publications/**nist**pubs/**800-63**/SP**800**-63V1_0_2.pdf*

APPENDIX A. Templates for Guiding Statewide Privacy and Security Frameworks

Template 1

HIE Architectural Model: Point-to-Point Directed Exchange

Domain	Description of approach and where domain is addressed in policies and practices	Description of how stakeholders and the public are made aware of the approach, policies, and practices	Description of gap area and process and timeline for addressing *(if needed, use additional documents to describe and insert reference here)*
Required to address			
Openness and Transparency			
Collection, Use and Disclosure Limitation			
Safeguards			
Accountability			
Optional to address			
Individual Access			
Correction			
Individual Choice			
Data Quality and Integrity			

Template 2

HIE Architectural Model: Data Aggregation (HIE entities that store, assemble or aggregate individually identifiable health information, whether centrally or in a federated model)

Domain	**Description of approach and where domain is addressed in policies and practices**	**Description of how stakeholders and the public are made aware of the approach, policies, and practices**	**Description of gap area and process and timeline for addressing** *(if needed, use additional documents to describe and insert reference here)*
Required to address			
Individual Access			
Correction			
Openness and Transparency			
Individual Choice			
Collection, Use and Disclosure Limitation			
Data Quality and Integrity			
Safeguards			
Accountability			