Core Services List

We propose to use NHIN terms to describe high-level services associated with data integration. The enclosed list is a sub-set of the longer and more extensive list of NHIN II objectives. Using this subset, we argue, confers the following advantages:

- It demonstrates a willingness to work with the federal government using their terms if not all of their priorities
- It focuses on some of the important matters while placing that which is less critical (e.g., direct consumer access to HIE data) in a more realistic context
- It should increase dialogue with NHIN II contractors and those who are following this effort. In Tennessee, CareSpark is participating in NHIN
- It allows regions and states to be more clear about the issues and to progress in an incremental fashion, keeping in context whatever is accomplished at the federal level.

These are suggestions – not policy. It is one approach that may help us understand

Abbreviations used in this document:

- CS-X – refers to NHIN II Core Services X where X is a number from 1-20. See: http://www.markfrisse.com/onc/core.html for the list and appendix A of the RFP for the definitions: http://fs1.fbo.gov/EPSData/HHS/Synopses/4607/07EASRT070057/RFP07EASRT070057.pdf
- G-A-X – refers to a specific annex (numbered 1-24) of the Gartner Group NHIN I report. See: http://www.markfrisse.com/onc/gartner-transactions.html
- G-5.3.X – refers to a common transaction (numbered 1-12) described in the Gartner NHIN I report. See: http://www.hhs.gov/healthit/healthnetwork/resources/summary_report_on_nhin_Prototype_architectures.pdf

Details of each are also provided as an appendix to this document. For more information, refer to http://www.markfrisse.com/onc

Near-Term Objectives

1. ***Delivery**. Secure data delivery, and confirmation of delivery, to EHRs, other systems and networks*[1] *(CS-1) [G-A-11] [G-A-13] [G-5.3.4] [G-5.3.5] [G-5.3.8] [G-5.3.9]*

   Summary

   - Delivery refers to an overall framework for sending and receiving data among different systems. It is largely an umbrella term to address the overall approach taken for physical delivery of data manner that ensures integrity, security, and audit capabilities.

2. ***Look up.** Data look - up, retrieval and data location registries (CS-2) [G-A-3]*

   Summary

[1] The NHIN core services emphasize heavily PHR and consumer services. These are out of scope of the initial interoperability discussions.

- Look-up refers to the ability to query an information exchange or system to determine if data are available for a specific individual.

3. ***Matching***. *Subject - data matching capabilities (CS-4) [G-A-1] [G-A-2]*

   Summary

   - This topic refers to the manner in which one tests and demonstrates that data are identified with the correct individual. Such demonstrations must take place both within an individual system and among systems exchanging data

4. ***Summaries***. *Summary patient record exchange (CS-5) [G-A-11]*

   Summary

   - Summaries refer to a means by which data authorized for review can be summarized and presented through a second system. The most common approach is to evolve toward a CCD architecture and to populate fields as systems make them available.

5. ***Integrity***. *Data integrity and non-repudiation checking (CS-6) [G-5.3.4] [G-5.3.8]*

   Summary

   - Integrity refers to the means by which data are ensured to be correct. Non-repudiation implies that the assertion of a data element at one time is not changed over time. If a data item is presented on day X and the data are later updated at a later date, non-repudiation capabilities imply that an inquiry will always demonstrate what was available at day X and not

6. ***Audits***. *Audit Logging and error handling for data access and exchange (CS-7) [G-5.3.1] [G-5.3.5]*

   Summary

   - One of the most pressing problems working across systems is the ability to ensure that data are used along the constraints set forth by participants. Audit logging within an exchange is a challenge. Audit logs across exchanges are undefined.

7. ***Choice***. *Management of consumer choices to not participate in network services (CS-13) [G-A-4]*

   Summary

   - In the case of MidSouth, this implies only the ability to "opt out" at the institutional level. As participation is broadened and multiple exchanges co-exist, there will be a need for setting generalized approaches across exchanges.

8. ***Identity***. *User identity proofing, and/or attestation of third party identity proofing for those connected through that HIE (CS-16) [G-5.3.12]*

   Summary

   - Generalized approach to identity management will have to be pursued. At present, a heavily manual "federated" approach is the rule where each exchange identifies its users and attests to this identity. These issues will become important as exchanges with different data use policies exchange information.

9. ***Authentication****. User authentication, and/or attestation of third party authentication for those connected through that HIE (CS-17) [G-5.3.2] [G-5.3.12]*

   Summary

   - MidSouth has taken a two-factor authentication approach to this. Other exchanges and repositories are taking different approaches. These must be reconciled.

10. ***Management****. Management of available capabilities and services information for connected user organizations and other HIEs (CS-21) [G-A-5]*

    Summary

    - This focuses on the notion of end-user support. Support is a real challenge given the many different points of failure and the complex chain of responsibilities.

11. ***Security****. HIE system security including perimeter protection, system management and timely cross – HIE issue resolution (CS-22) (not primarily related to interchange capabilities)*

    Summary

    - This focuses on both systems security and non-interchange-related system concerns

12. ***De-authorization****. Temporary and permanent de-authorization of direct and third party users when necessary (CS-23) [G-A-2]*

    Summary

    - One issue arising in Wilson county and elsewhere exemplifies this service. What are the responsibilities of an organization to alert an exchange that use by a third party is no longer authorized? How is this propagated? How is this documented?

Long-term Objectives

1. Support for notification of the availability of new or updated data (CS-3) [G-A-13] [G-A-14]
2. Support for secondary use of clinical data including data provisioning and distribution of data transmission parameters (CS-8) [G-A-6] [G-A-8] [G-A-9]
3. Data anonymization and re-identification as well as HIPAA de-identification (CS-9) [G-A-9][G-5.3.6]
4. Management of consumer identified locations for the storage of their personal health records (CS-10)[G-A-9]
5. Support of consumer information location requests and data routing to consumer identified personal health records (CS-11) [G-A-2] [G-A-14]
6. Management of consumer-controlled providers of care and access permissions information (CS-12) [G-A-4]
7. Support of a HIE-level, non-redundant methodology for managed identities (CS-20) [G-5.3.12]
8. Subject and user identity arbitration with like identities from other HIEs (CS-18) [G-A-1] [G-A-2]
9. Consumer access to audit logging and disclosure information for PHR and HIE data (CS-14) [G-A-7]
10. Routing of consumer requests for data corrections (CS-15) [G-A-12]

11. Management of user credentialing information (including medical credentials as needed to inform network roles) (CS-19) [G-5.3.12]
12. Emergency access capabilities to support appropriate individual and population emergency access needs (CS-24) [G-A-4]

Appendix

Gartner Common Transaction Features[2]

- Audit Logging (Gartner 5.3.1)
- Authentication (Person) (Gartner 5.3.2)
- Authentication (System) (Gartner 5.3.3)
- Data Integrity Checking (Gartner 5.3.4)
- Error Handling (Gartner 5.3.5)
- HIPAA De-Identification (Gartner 5.3.6)
- Holding Messages for secondary use (Gartner 5.3.7)
- Non-repudiation (Gartner 5.3.8)
- Patient Summary Record Support (Gartner 5.3.9)
- Pseudonymize and Re-Identify (Gartner 5.3.10)
- Secure Transport (Gartner 5.3.11)
- Transmit Disambiguated Identities (Gartner 5.3.12)

Sets of Interchange Capabilities (Annex Issues)

- Arbitrate Identity (Gartner Annex 1)
- Identify Subject (Gartner Annex 2)
- Locate Records (Gartner Annex 3)
- Maintain Consumer Data Sharing Permissions (Gartner Annex 4)
- Maintain Registries of NHIN-Participating Systems and Organizations (Gartner Annex 5)
- Manage Data Selection Parameters for Secondary Use (Gartner Annex 6)
- Provide Consumer Access to Access and Disclosure Logs (Gartner Annex 7)
- Provide Data to Secondary Users (Gartner Annex 8)
- Pseudonymize and Re-Identify Data (Gartner Annex 9)
- Publish PHR Location (Gartner Annex 10)
- Retrieve Data (Gartner Annex 11)
- Route Consumer Request to Correct Data (Gartner Annex 12)
- Route Data (Gartner Annex 13)
- Route Data Based on Consumer-Specified Preferences (Gartner Annex 14)

[2] 1. Gartner Group, *Summary of the NHIN Prototype Architecture Contracts*. 2007, HHS, Office of the National Coordinator for Health IT: Washington.