JASON Report Task Force Listening Session

Written Testimony to accompany and elaborate-on the verbal testimony of Eric Heflin

Presented 2014-July-31

Good afternoon, for my 5 minute speaking opportunity, I'm going to hit the highlights of a more comprehensive written testimony I've also submitted. Due to time constraints, I'll be unable to drill down in to the details, but have provided those in written form, including references. Underlined text was presented verbally.

My remarks are to provide a little bit of additional perspective on several key JASON report topics, with some more specifics regarding the viability of these topics.

I believe the single most important topic that would need extension to make a JASON-like design work is not a technical item, it is a legal, policy, operational and trust framework. The eHealth Exchange DURSA enables this and avoids to the need to establish point-to-point agreements. Point-to-point agreements do not scale.

The JASON report suggests for a common mark up language be created to facilitate interoperability. Today we have a markup language called the CDA (Clinical Document Architecture), and more specifically the Consolidated-CDA. C-CDA does a good, but not yet complete tagging of clinical data. Capabilities include highly structured data exchange, controlled vocabularies, ability to be tested to a large extent to ensure conformance, MU2 sanctioning, increasing vendor support, and good patient demographics for accurate patient matching. C-CDA interoperability gaps do exist though, and I've detailed these more in my written testimony. Gaps, though, include lack of support universally today (although this is being resolved through 2014 I believe), lack of detail in some areas such as exact location and rules about where certain types of clinical information are to reside, virtually no interoperability of the free-form text component of the CDA document, lack of implementation toolkits for creating, parsing, and quality assuring these types of documents. In addition, C-CDA is intent to covey a "snapshot" of patient's record; not a continuous stream of information such as from a medical device. A new, effort called Fast Health Interoperability Resources (FHIR) is currently gaining interest. And may become the successor for C-CDA. My recommendation is for us to globally invest in C-CDA, remediate the known gaps, create viable tooling to author, manage, and test C-CDA. And for us to monitor FHIR, to see if it indeed is simpler than C-CDA.

JASON recommends a semantic translation layer, but it envisions that layer residing between the data and the users of those data. I believe there is a role for dynamic semantic translation, but it's limited. Specifically, semantic translation is rarely perfect, leading to a incorrect translation. Often, the only location in the data workflow where semantic normalization to standard value sets can be accomplished is at the source of the data. Also, translation is expensive in terms of QA. My recommendation is to perform this semantic translation one-time for each data source, at the source or at least before it is written to the durable storage location. The added benefit of this approach, is that it also allows the raw data to be used for analytics and research with no additional semantic translation. Many high quality, expressive, and sufficient vocabularies exist now that can be leveraged. Many of these vocabularies have been recognized by MU and provide a single target for the industry. My recommendation is that we continue to leverage these vocabularies, and ensure they can be curated in public and transparent manner over the years to come, and to perform the semantic normalization at the source of the data.

JASON advances the concept of a "privacy bundle". Some of the concepts related to giving patients control over groups of their data are viable today, with some very promising targets on the short-term horizon. And ONE/IHE joint initiative, called DS4P (Data Segmentation 4 Privacy) indeed is nearing completion as true standard that will allow patients to express certain consent preferences, and those preferences can be carried with the data in the form of an obligation so that any future person or computer that views the document has a clearer understanding of the patient preferences. Today, the eHealth Exchange is in production with another standard called BPPC that allows a patient's authorization for SSA claims to be sent along with the

request. This allows the disclosing party to decide if they will honor the request. Other standards also exist, including HL7 "Consent Directives", OASIS with a standard called XACML, that can also be used to express patient privacy and other preferences in a manner that can be understood by a human or a computer. My recommendation is to select a national target for automatable consent, and leverage existing standards to convey that expression.

JASON recommends an "API" to allow obtaining data from EMRs. I too personally feel that there is a significant impediment to wide-scale healthcare information exchange due to EMRs. However, the issue is not a technical one as much as it is a business one in that may have expressed to me that the EMR pricing model is not acceptable. MU requires that EMRs provide the ability to export and consume CDA documents. But there gaps in the CDA standards, as mentioned above, that make it somewhat difficult to interoperate, and in many cases the CDA documents are incomplete (absent critically important patient information such as current medications, allergies, etc.). We do have some positive examples though. Some EMR vendors have shown and taken to market products that are actually interoperable. They support open industry standards such as XDS, XCA. In addition, a new ONC-lead initiative, that is now in the process of becoming an IHE standard, called Data Access Framework (DAF) is nearing completion and will provide a target for a JASON-like API on top of EMRs to allow the EMR data to be opened up for access under secure conditions. It's notable that DAF recognizes and re-uses existing standards. The DAF is intended to enable queries within and across enterprises, queries for both individuals and populations of patients, support for multiple data models such as patient, provider, clinical, storage of data in multiple systems, and security. In addition, the eHealth Exchange is live today with an API called XCA that allows access to patient or claimant data using an open standard. We currently have 72 organizations live using the XCA "API" which represents access to close to 1/3 of all patients in the USA. We have a number of positive and negative experiences to share, over the 5+ years since the ONC initially created us. The DoD and VHA are mentioned in the JASON report, and are already a part of the eHealth Exchange, along with the SSA whom has seem claim turn around times plumit via the use of electronic record exchange via the eHealth Exchange. My recommendation is to continue using this proven "API" standards, and to work together as an industry along with government to improve them.

The JASON reports briefly mentions patient matching as a concern. I too feel this is a looming issue on the industry. Matching inside organizations is tough. Matching across organizations is significantly more difficult, as we are seeing in production today. The solution, I feel, in the absence of a national identifier, is to clarify matching best practices and minimal acceptable practices. The CCC and eHealth Exchange are nearly complete publishing a white paper, informed by our years of production experience and the strong support of Intermountain Healthecare, documenting dramatic improvements that can be achieved in terms of patient matching via implementation of a dozen or so minimal acceptable practices. In the future, I expect that the eHealth Exchange will publish this as non-binding guidance, and then later make it policy, and then finally, test for it as a condition for membership. My recommendation is that we continue as an industry include minimal patient matching guidance in our best practices.

The JASON 'middleware' architectural layer is where one standards body, the IHE International Information Technology Infrastructure, has been focusing for many years. In addition, through periodic international Connectathons, the IHE facilitates a peer-to-peer testing process to assess actual interoperability. In the near future, IHE International will also over a formal testing and certification program to provide independent 3rd party verification of interoperability in specific products. My recommendation is to review the standards published by the IHE ITI committee as many of the JASON concepts have already been released as public standards.

Key management in JASON has some challenges, such as providing keys to access data, and the significant burden of actually installing certificates. But a similar approach IS viable, provides identical benefits in terms of strength of encryption, which is call access control based on roles, purpose of the transaction, context such as DR, or other attributes or information. We are in production today with this in the eHEx, and I'm aware of multiple other, highly vible and effective, implementations in the HIE and EMR space. Standards such as SAML, XUA, and the eHEX Authorization Framework are in production today with most of the JASON "key

management" concepts, including encryption at all times, using of PKI and open standards, authentication of both parties to the exchange of clinical data, privacy protection, and audit logging. In addition, XUA allows the disclosing party to make an access control decision informed by the context of the request such as the purpose, any associated patient authorization, the role of the requester, etc. The eHealth Exchange has managed a PKI for 7+ years now, and has learned many lessons learned regarding the viability of deploying certificates at the scale of several hundred systems. One important lesson learned is that installing certificates is difficult, even for IT professionals. The JASON key management is already in production use, almost exactly as described by the JASON report, and is handled by the lower level "2-way-TLS" employed by the eHealth Exchange today. Specifically it is used for mutual authentication of the authenticity of each party to the exchange, plus it encrypts the pipe so data is not readable, and more.

Regarding crypto, it is indeed sufficiently efficient in terms of computer processing, but it remains difficult and expensive in terms of human training and use. How many can generate their own personal x.509 certificate, install it, properly administer it, and then share it? Can you imagine all members of your family performing these actions? Today, I estimate it takes an IT professional an average of 1 full day to install a PKI x.509 certificate when you add training and diagnostic issues. PKI does work, but the effort is not small and needs to become easier. Tools and common procedures to assist are being sporadically developed.

One benefit to a PKI use, is that it reduces the ability of hackers to access patient data. But it is far from being sufficient. My recommendation is that any national approach conduct a threat/risk assessment for that architecture to ensure all threats of concern have an acceptable mitigation. Ideally, such an analysis should be conducted prior to the creation of an architecture since security requirements can drive architectural changes. The eHealth Exchange conducted such an analysis before the requirements or architecture were finalized, and help inform our current operational model. For example, one threat we were concerned about was replay attacks. Our mitigation was to include a signed timestamp in the clinical message exchange. My recommendation is to ensure that industry conducts formal and complete risk assessments during the requirements gathering phase to help ensure security is designed in, not bolted on.

On missing element in the JASON report is the process of identity proofing patients so we know the right person is exerting control over their record and preferences. National efforts like NSTIC are promising approaches to allow large numbers of patients to be identity proofed and more strongly authenticated.

In conclusion, I feel that many of the JASON elements are viable and in production today. Other elements are laudable goals that should help inform the national agenda in terms of requirements to consider, vet, and act on as is needed.

S&I Framework Data Access Framework

http://wiki.siframework.org/Data+Access+Framework+Homepage

IHE Data Access Framework

http://www.ihe.net/uploadedFiles/Documents/PCC/IHE_PCC_White_Paper_DAF_Rev1.0_2014-03-28.pdf

A Robust Health Data Infrastructure "the JASON report"

http://healthit.gov/sites/default/files/ptp13-700hhs_white.pdf

National Strategy for Trusted Identities in Cyberspace (NSTIC)

http://www.nist.gov/nstic/