

Standards Lessons from the Web

Following last week's HIT Standards Committee [Implementation Workgroup Hearing](#), Microsoft's [Sean Nolan](#) and Gartner's [Wes Rishel](#) wrote thoughtful blogs.

They point out that the web has two basic standards - content (HTML) and transport (HTTP). Of course there are several other supporting standards such as DNS, TLS/SSL, URL syntax, CSS, etc. but to get started all you need is basic content and transport. You can learn everything you need to know to create a web page in under an hour.

At the hearings, I got that sense that much of the content we've (HITSP, HIT Standards Committee, the industry in general) proposed for healthcare such as NCPDP Script for eRx, HL7 2.x for lab, and X12 for administrative transactions is fine. There is some debate about the right level of simplification for a clinical summary standard, but I'm convinced that the SDOs will continue to refine clinical summaries in a way that ensures suitable content packages will be available for simple and complex use cases. There is additional vocabulary work to do, but that is already in progress.

On the transport side, let's explore the options:

1. Do nothing and let the market develop a transport mechanism - after all that is what happened with HIPAA (it specified the content as X12 4010 and left implementation of transport up to the market)

I do not favor this option. In Massachusetts, [NEHEN](#) implemented secure appliances to solve the problem of data transport. We spent millions and took years to do this. HIPAA transactions are not as widely implemented as the industry would like, largely because transport standards were missing and implementation guidance for the content was not detailed enough. Of course, you could force everyone to sign up for the clearinghouse/intermediary of their choice but this creates heterogeneity, click fees, and unnecessary middlemen.

2. Specify all the standards and policies necessary for end to end secure transport.

Thus far, we've stayed architecturally neutral and provided a suite of standards for transport that ensure authentication, authorization, role-based access control, and auditing to support all policy variations. This approach has been a fine starting point, but it needs to be refined via policy so the number of standards can be constrained. For example, a policy which states that audit trails must be available showing who looked at what when is probably sufficient instead of requiring every organization to implement a standards-based audit trail. It's unclear what the business case is for a completely standardized, interoperable audit trail. Another example - If policy requires segmentation of the record into standard care, HIV care, mental health care, and substance abuse care, as well as requires that the application enables patients to record their preferences for release of these 4 segments, do we need access control standards or accept that the application adequately protects privacy?

If policies and certification ensure appropriate application behavior then point to point transport might be as simple as TLS with bilateral certificate exchange at the infrastructure level, substantially reducing the burden of implementation.

Of course, some may argue that an approach that uses simple web standards for securing transmission and leaves other privacy controls to the application cannot ensure "chain of trust" end to end security. It is true that each organization and stakeholder would have to decide if they trust the applications used by their trading partners. Our experience with NEHEN is that policy, [data use and reciprocal support agreements](#) (DURSA), and simple transport standards can facilitate rapid implementation of healthcare information exchange.

3. Deploy appliances that serve as secure gateways between organizations.

With policies and over the wire security standards, the market can develop appliances that securely transport packages of content. Some may be SOAP-based using CAQH Core or XDS/XDR and some may be REST-based. The folks at [FHA Connect](#) have done a great job creating an open source application that can serve as such an appliance.

One thing I've learned from negotiation (my [Walks in the Woods](#)) is that being dogmatic about one solution is rarely the right answer. Folks who know me often hear the word "parsimonious" - the smallest number of solutions needed to meet the needs of stakeholders. The answer is not 100 variations but a small number that provides business value - the right tool for the right job. From the work I've seen thus far, I think the transport solutions that will work for stakeholders include:

1. For those who want end to end standards controlled secure transport that guarantees integrity of documents - XDS, XDR, XDM and XCA fulfill the need. These standards are SOAP-based and enable use of WS* security controls, so they are useful for protecting privacy at the standards level.

2. For those who want standards-based security with simple implementation, an appliance such as FHA Connect, NEHEN, Intersystems' Ensemble, or Orion Health's Rhapsody is a very reasonable approach.

3. For those who want a secure channel for transporting data elements such as a problem lists, medication lists, and labs from EHR to PHR, a simple TLS and REST approach is good enough. Ideally, HITSP and the HIT Standards Committee workgroups will provide an implementation guide with standard URIs/querystrings so that we'll not have huge variation in REST APIs. Some have used the term "Healthcare Internet" to describe such an approach.

I look forward to the work of the next several months. I'm confident that HITSP, the HIT Standards Committee Workgroups, and the new HIT Policy Committee NHIN Workgroup will evaluate the options and make recommendations.