Comments to the API Task for of the HIT Policy Committee
January 28, 2016
John Moehrke, Principal Architect, GE Healthcare

I want to thank the ONC "API Task Force" for inviting me to speak on behalf of GE Healthcare, as one of the representatives of the Vendor community presenting on January 28th.

I am a Principal Architect specializing in Standards Architecture in Interoperability, Security, and Privacy for GE Healthcare. I've been primarily involved in international standards efforts related to GE's healthcare businesses. I am a co-chair of the HL7 Security workgroup, and a member of the FHIR Management Group (FMG). I am also a GE representative to DICOM, HL7, NEMA/MITA, ISO/TC-215, and IHE. In addition, I am active in many regional initiatives such as the S&I Framework, HEART, NwHIN-Exchange, and WISHIN. I am currently working on the FHIR and IHE efforts to support APIs to Health Information Exchange(HIE) through the development of the IHE-Mobile Health Documents (MHD) profile which created the FHIR DocumentReference and DocumentManifest; and through FHIR Privacy and Security and HEART efforts to support Patient Privacy Consent Directives. I have been active in Healthcare standardization since 1999, during which time I have authored various standards, profiles and white papers. I blog at http://healthcaresecprivacy.blogspot.com/

GE Healthcare is and has been a strong supporter of standards-based Interoperability. This commitment is reflected in our active participation and leadership in healthcare standards like HL7, DICOM, ISO, ASTM, and IHE; through our participation in general IT standards organizations like IETF, W3C, OASIS, and our extensive use of open standards across our product portfolio. Finally, I am an active participant and advocate for the HEART workgroup as an example of a cross-domain group including experts from the OpenID Connect, OAuth, and UMA domains; working with those from the healthcare domain to align on focused profiles.

I have been asked to address several questions, which I will do at a summary level today

The questions I have been asked to address are:

1. Does your organization use APIs for apps that are available internally or to third parties? If so:
    a. Are they clinician facing, or consumer facing (or both)?
    b. Do you publish your documentation online or make it available to third party developers?
        i. How do you determine who can get access to it?
        ii. Do they need to be "certified" by your organization to use?
    c. Are there terms of use that include specific language for privacy and security?
2. Are there production deployments of these APIs/third party applications using APIs?

3. What are the perceived and actual privacy concerns or barriers to the adoption of APIs?
4. What are the perceived and actual security risks or barriers to the adoption of APIs?
5. Are there third party certifying authorities in non-healthcare industry that we can leverage?

APIs available

GE Healthcare has had APIs as part of our systems for decades. Most of these are the bread-and-butter of any healthcare organization's network backbone, drawing on HL7 and DICOM, using IHE Profiles. We use HL7 for Patient identity, Orders, Observations, Lab results, etc.; and DICOM for all things imaging, including CT, MRI, X-Ray, Ultrasound, etc. We design these APIs using IHE profiles to drive robust interfaces, yet also have flexible configurations to customize to the local clinic flavor of these protocols. Using such internationally recognized standards allow GE Healthcare to focus on the international marketspace while also meeting needs of local healthcare providers. The ability to use global standards allows us to re-use the same solutions.

Many of our IT products have had web friendly APIs for some time. These have generally been focused on providing a way to view information from another system. These web-friendly APIs are mostly a browser (HTTP/HTML) interface that is based on URL parameters to invoke a web session. This process starts a web session that can be invoked by any application given some context such as user, patient, order, time-frame or study.

GE Healthcare also supports Web interfaces intended to be used by Patients, via multiple patient portals that use APIs to access information from our EHRs. In addition to more generally meeting the needs for enhanced patient engagement, this functionality supports the Meaningful Use capabilities for View, Download and Transfer.

These existing APIs, and similar API use across the industry, clearly have security implications that we have had to address. Most importantly for today's hearing, broader use of APIs, likely focused on HTTP/RESTful APIs, such as HL7 FHIR, and DICOM WADO/QIDO/STOW, will present a robust set of security and privacy issues. Like the industry generally, GE is in the early stages of working with these newer APIs and welcomes the insights that will be generated by this task force.

API accessibility

APIs that are using interoperability standards like HL7, DICOM, and IHE are available for use by our customers. Often, the customer wants us to customize the API or interface to their local dialect of the applicable standard. We have a robust service organization to assist customers with such customization. Where a customer has programming capability, they can access the documentation of the API and leverage it to best meet their needs. We place no special qualifications upon our customers to gain access to the API. There is a need for caution, of course, by developers and providers and others you use APIs as any use of an API can have quality and safety impacts on a system.

API use today

Clearly there is ubiquitous use of HL7 v2, HL7 CDA, DICOM, and IHE; but I suspect that the API task force is more interested in HTTP/RESTful API use. We are considering future products that I have been actively involved in that may use newer APIs. I will focus on applicable API issues for the remainder of the questions, drawing on the range of my experience with legacy and newer APIs.

Perceived and Actual Privacy Concerns

Privacy concerns mostly involve shared roles and responsibilities between healthcare provider organization and GE as the vendor providing the system. Given that GE doesn't have direct relationship with the patient, where the provider organization does have a relationship with the patient and controls the policies and use, the privacy concerns must fall to the provider organization. Given this reality, we do have a Privacy-By-Design approach built into our product development processes. This approach presents the product team with a set of Privacy-By-Design scenarios, guiding them to provide privacy capabilities to the healthcare provider organization. This process includes the capability to follow patient consent directives and record privacy relevant events.

Perceived and Actual Security Concerns

The main problem that we see is the very wide variation in security and privacy maturity of healthcare provider organizations. The very large organizations have mature capabilities and have policies, procedures and technology solutions available on which we can build a trust relationship. The vast majority of healthcare provider organizations, however, don't yet have the full range of these operational aspects; this situation is especially relevant to public policy given the API requirements set out in the 2015 edition certification requirements and the associated Meaningful Use Stage 3 provisions.

Certification

GE Healthcare does not have information on certifying bodies in other industries to leverage in this context. What is important is that any certifying body must be able to address policy, procedure, and technology. Focus on technical certification alone will not bring the level of maturity needed. In general, however, we urge caution in the use of additional certification requirements in this emerging area of technology and review of other methods to address needed actions by vendors and providers.

Enabling Technology for Security and Privacy

In this section, I address specific enabling technologies used to enhance security and privacy.

1. User Identity and Authentication Management – Healthcare software, especially APIs, should not include its own identity management and authentication system. It should, instead, hook into a healthcare organization managed Single-Sign-On (SSO) infrastructure. Thus the hospital or other organization provides access to User Identity and Authentication Management as a service. This approach is what the OpenID-Connect using OAuth and SAML standards define.

   A good Federated Identity Management system provides security "claims" that the relying software can use to correlate users to roles and responsibilities. There are some large hospital systems deploying an SSO solution, but they generally have not yet created policies or procedures on how to connect external software or new systems to that SSO solution. The

majority of healthcare provider organizations, however, do not have a SSO system; thus any new software adds more user login credentials that are not coordinated. IHE Connectathons are working to test the IUA profile, which profiles OAuth for this purpose.

2. Security and Privacy Audit Logging – Healthcare software, especially APIs, should not add another audit logging system, which would propagate multiple uncoordinated logs. Rather, the API or other software should catch all security and privacy relevant events, but should then leverage an external service or solution to report these incidents to for log management, analysis and reporting. Few large hospitals have deployed an audit log service; those that exist tend to be focused on firewall, antivirus, and intrusion detection and are not mature enough to handle healthcare software level logging. An audit log service should support authenticated audit entry sources using either SYSLOG, ATNA, or FHIR AuditEvent. IHE Connectathons test for IHE-ATNA capability today.

3. Cloud services, mobile applications and medical devices all need to be strongly authenticated to other systems within the healthcare provider organization. This authentication is done by issuing a system or machine identity using Non-Person-Entity (NPE) management system. Some NPEs are associated with a person, such as a personal measurement device. Many NPEs, however, are standalone systems that are not associated with a person. For those NPEs associated with a person, OAuth credentials can be issued [to that person.

   Many systems, especially cloud systems or medical devices, need to have identities issued to the software or device and managed independent of any person. For these NPEs, a digital certificate may be the best approach, especially for long-lived identities. For other use-cases, a service identity (client_id) would be issued from the OAuth identity manager. Few large hospitals or other large healthcare organizations have selected a Certificate Authority, either under their own management or under contract. Fewer have an OAuth infrastructure. These robust security services need to be more widely available and it is essential that the healthcare organization or system has a policy and procedure to assure that identities are issued to NPEs only after justification, inspection, and monitoring.

These are the large problems. In the absence of these needed security approaches, proliferation of user login credentials and non-coordinated audit logs make the work of the healthcare organization Privacy and Security office very challenging with respect to healthcare software.

In my role as Security WG co-chair and IHE/HL7 liaison, I am leading an effort in HL7 to create a FHIR Implementation Guide on Document Sharing Health Information Exchange. Within this work, we intend to apply these technologies toward a Health Information Exchange overall workflow. This effort will encourage and leverage cooperation between IHE, HL7, and HEART, and any organizations that want to participate.

Policy and Procedure as Enablers of Security and Privacy

There is a next level of policies, procedures and actions needed once the above fundamentals are in place. These include:

1. Defined Roles and Responsibilities around Security/Privacy monitoring, incident reporting, and remediation.

2. Defined Roles and Responsibilities around Patient Privacy enabling: Consent gathering, Consent enforcement, Accounting of Disclosures, Access and Amendment, and other communications.
3. Clarity on how the patient is verifiably identified and ensuring that the Level of Assurance is good enough to assure that the patient access is really by that specific patient; while not making it impossible for patients to access their own data.
4. Use of consumer-based identity providers such as Facebook™, Google™, Twitter™, etc. present identity-proofing issues. There is a need to come up with a universal policy for how these services can be used by consumers, while the Identity Level of Assurance is elevated to an acceptable level for access to a person's own healthcare information.
5. As a part of system identify/authentication
    a. Apps need a infrastructure for registering as a trusted participant on an API. This registration needs to be backed by Policy and Procedure.
    b. We need means for providers to learn to trust an app. This capability needs to address both a technical registry of applications that have been vetted by some authority, as well as a mechanism to address how we all gain trust over the vetting organization.
    c. We also need a similar means for patients and consumers to learn to trust an app.
    d. When that trust is broken, we need incident response mechanisms, and remediation mechanisms.
    e. We need to recognize and respond to the fact that a broken trust in healthcare is exposure of personal information that is not-revocable (unlike other industries).
6. Patients and consumers need to be allowed to Create or Update data, actions that present "Provenance" and "Trust-Integrity" issues that must be resolved.
7. Acceptable Services need to be identified.

Conclusion

Thank you for the opportunity to provide our perspectives today. GE Healthcare is dedicated to the development and use of globally recognized interoperability standards, which are the basis of all our technology choices.

In my concluding remarks, I'd like to emphasize that these technology standards are not the focus of the challenges in bringing HTTP/RESTful APIs to our customers, which tend to be primarily about policies. Such policy issues focus on the roles and responsibilities for the various requirements regarding privacy and security operation: Identity Management, Authentication, Consent, Accountability, and Incident Management. These are types of Policy and Procedures that we often don't find at healthcare organizations.

- Patient Identities are an especially problematic area of identity management. With no controlled Patient Identity, privacy cannot be managed or assured. This challenge applies to data management, consent management, and patient access management.

- User Identities need to be managed by the healthcare provider organization. The healthcare provider organization must take responsibility for the functionality of User Provisioning, user De-Provisioning, Authentication, Account Recovery, Account Suspension, Account Deletion and Account Monitoring. Vendors and applications can leverage the use of standards like OpenID Connect using OAuth.

Overall, the security and privacy challenges associated with APIs reflect and are a consequence of the wide variety of maturity of healthcare provider organizations in both policy and technology. These challenges clearly need effective and timely consideration given the current policy drivers to braid and deep API use in healthcare. Thank you.