EMR Direct
SIMPLIFYING INTEROPERABILITY

Move Health Data Forward Challenge Phase 1 – Proposal

September 8, 2016

Executive Summary

EMR Direct's HealthToGo™ Interoperability Engine will improve the accessibility of patient health data by facilitating the deployment of APIs through easily-enabled software that supports scalable provisioning and consumer-mediated exchange. This framework, based on the HEART profiles, is designed for optimal user experience and efficiency, and allows the discoverability of identities and resources through a federated approach to identity management.

Both patients and users they authorize are expected to benefit from the HealthToGo platform, as well as healthcare providers that want to deploy an API or want to federate identities used with APIs they have already deployed, and client app developers seeking to deploy apps that can easily integrate patient data from multiple data holders using APIs.

The specific problems being solved by EMR Direct HealthToGo Interoperability Engine include:

- Exposing a public API as a service on behalf of data holders, to enable data access by data owners and their grantees through the HL7® FHIR® standard
- Enabling additional APIs and underlying services for consumer-mediated authorization and authentication, including:
    - Implementing an Authorization Server that leverages the HEART OAuth 2.0, OpenID Connect, and User-Managed Access (UMA) profiles
    - Extending the OAuth 2.0 profile to encapsulate UMA entitlements and other helpful identity information
    - Implementing a Client Token Service (CTS) that can be used as part of a trusted network for sharing identity information and digitally signing tokens
    - Development of federated profiles that may be used by other entities to stand up similar infrastructures
- Providing user registration and Identity Verification services, including Individual and Organizational identity, and binding user identities to reusable credentials
- Providing documentation and terms as required for certification of HealthToGo Interoperability Engine for 170.315(g)(7-9)
- Enabling HIPAA compliance by service customers and application developers bound by HIPAA

EMR Direct Background

EMR Direct is a Healthcare IT company located in San Diego, California. Since its launch four years ago, our phiMail® Direct Messaging platform, including our Direct Messaging integration API, has been selected by 1 in 3 EHR vendors certifying for the Direct-related measures (Transitions of Care; Patient View, Download, Transmit) in the 2014 Edition ONC criteria needed for Meaningful Use. This full-featured, robust, developer-friendly solution was developed and brought to market by our in-house US-

based team. Using development resources and in-house clinical and software development expertise already in place, we intend to provide another developer-friendly product, with Application Access and other interoperability services included in the HealthToGo platform. We also have existing infrastructure for identity management in place as we currently operate a full service Certificate Authority and Registration Authority to support health information exchange.

EMR Direct's company mission is to simplify interoperability and enable custom workflows, through technology that is easy to deploy and does not require expensive, one-off, peer-to-peer interfaces. Our management team has taken on multiple leadership roles in ONC's Direct Project and DirectTrust workgroups, participating in the authoring of documents such as the Trust Bundle Distribution Guide, Implementation Guide for Direct Edge Protocols, DirectTrust Certificate Policy and HISP Policy, and Direct Project Applicability Statement version 1.2. Most recently, EMR Direct developed the Unified Data Access Profile (UDAP) for leveraging digital X.509 certificates to help scale the use of APIs and provide added identity assurance to API-based data exchange.

Introducing HealthToGo Interoperability Engine

In developing our API platform, we anticipated scalability challenges in production if identity management and authorization grant management could not be federated as part of this ecosystem's design. As standards are falling into place for enablement of an Application Access ecosystem, there is potential to fall back to an expensive custom interfaces model, introduce gaps in security, or even a semblance of information blocking if Application Access is not properly executed. EMR Direct's vision for scaling authorization and authentication to APIs involves reusable credentials incorporated into the proposed OAuth framework for FHIR, where efficient to do so. For this reason, we have developed a solution that leverages the same type of robust security and trust framework and trust in identity that is already in place for Direct Messaging networks. We have solutions that step a new user up to a higher-assurance credential when needed, that leverage existing credentials for health information exchange when available, and that use a Public Key Infrastructure (PKI) across healthcare providers or identity provider services to generate an OAuth-style token for use in federated or non-federated scenarios.

As with our Direct Messaging business model, cost to healthcare organizations who enable Application Access with the HealthToGo platform will be much lower than their potential outlay and ongoing investment to replicate in-house the necessary subject matter expertise and infrastructure, since there are significant economies of scale in deploying this specialized infrastructure for use by many organizations simultaneously. Healthcare organizations and Health IT vendors deploying our solution will therefore require relatively low technical investment in order to implement the HealthToGo platform.

For pricing, we expect to take a similar approach to that of our Direct Messaging business. Our costs to provision services are proportional to the resources used to host services for each additional healthcare organization, and are proportional to number of providers at the organization. Therefore, we charge less for small practices and scale up for larger organizations. We offer metered pricing for use cases that exceed expected resource levels or do not fit the typical ambulatory or acute care settings. A small setup fee covers our one-time costs in the initial onboarding of a healthcare organization. Development and expansion of technical infrastructure will be primarily funded from existing operational revenue. Phase 1 challenge grant funds will be allocated to provide administrative resources to run our complimentary developer sandbox program for the HealthToGo platform. Subsequent phases would be allocated to purchase hardware and provide additional developer support resources.

We expect the software as a service model will be well-received for APIs, since it can be burdensome and therefore costly to healthcare organizations to enable secure access to Protected Health Information (PHI). Of course, there are the additional policy advantages to our model since the expense of procuring N-squared one-off legal agreements, repeating identity proofing events, and duplicating client registration and user registration for every distinct data holder resource and all users and authorized access grantees is also minimized.

EMR Direct demonstrated a prototype of this solution at HIMSS 2016, and expects that the security and infrastructure requirements of operationalizing the service will be similar to our experience in onboarding and servicing our Direct Messaging customers, and that this service can be successfully deployed through our existing channels. Our team understands the challenges and possesses the resources and expertise necessary to deploy the data access and resource authorization and authentication protocols necessary to service API access and grant management at scale.

Interoperability is important to EMR Direct, and we expect our customers will also value information liquidity as a means to improve quality of care. For this reason, we have been and will continue to participate in HEART, Argonaut, and other workgroup discussions that are framing the ecosystem for Application Access. EMR Direct already operates as a HIPAA-compliant service for Direct messaging and the same infrastructure will be used for the HealthToGo service. We are already running other production services that leverage OAuth 2.0, and have developed in-house expertise in that subject. EMR Direct not only has a history of successfully operationalizing these important standards, but we also have a deep understanding of the regulations behind them that guide ongoing practices and of industry recommendations toward developing new conventions.

Technical Details

The HealthToGo Interoperability Engine is being developed to achieve the objectives listed in the Executive Summary using the HEART profiles for OAuth 2.0, OpenID Connect, FHIR OAuth 2.0 Scopes, and UMA.

Part of the HealthToGo platform involves pre-built “app” web pages in HTML5, hosted by EMR Direct and accessible via browser on a PC, tablet or smartphone, to maximize the accessibility by consumers using the technology of their choice. These pages comprise a web application that serves not only as a conventional OAuth 2.0 Authorization Server used by FHIR clients to access health data, but also as a client app and user interface to configure user-managed access in our authorization and authentication framework.

Development Plan

Work on extending authorization via the HEART profiles for HealthToGo is already in progress. Our existing OAuth 2.0 Authorization Server technology and FHIR RESTful server technologies are being adapted to implement these profiles. Remaining tasks involve the real world testing, customer feedback, and posting documentation and terms.

Extending HEART

The proposed solution would enable APIs for Application Access based on our existing FHIR server technology and would incorporate the use of UDAP where it increases the scalability of establishing trust in identity as a means for authorizing users to access health data. UDAP provides a framework for signing Java Web Tokens (JWTs) for OAuth 2.0 authorization and/or authentication actions using digital certificates, and is compatible with the HEART profiles. The management of the certificates is federated so as to eliminate a separate registration with every Resource Server for every API user or client application. This is a variation on the public key distribution model in the OpenID profile and in RFC7517. This enables reuse of existing trusted network of digital certificates that are already used to secure other health networks, such as in Direct Messaging. The value to the community is in the reuse of identity proofing events, proofing artifacts, and digital certificates.

We see advantages to additionally enabling an OpenID UserInfo endpoint in order to share information about a user from a trusted CTS to an UMA-enabled Authorization Server that accepts JWTs from that CTS. Such a model would facilitate matching by enabling a user's one-time registration with an identity provider that can be queried by participating Authorization Servers to make access decisions and by data owners to make entitlement grants. By appointing such trusted identity providers to bind access rights to a specific identity at the time that they are granted, the client authorization process can be streamlined. A subsequent data access request might include an authorization token referencing the appropriate grant event, streamlining the number of OAuth redirects necessary to generate an access token or RPT.

To illustrate this example, a CTS may accumulate grants to various resources, which the CTS records as they are granted by the data owners, and present metadata from these grants to the user to assist the user in finding the associated API endpoints. Then, when the user attempts to access that data, the user's CTS might securely transmit a digitally signed token to the resource holder's UMA-enabled Authorization Server representing that user's access grant to these resources by the data owner. The token binds the user's identity at the user's identity provider to a grantee referenced by the UMA-enabled Authorization Server where the data owner has made the grant. Thus, after validation of such a token received from a trusted CTS, validation that the grant to the requested resource is still active in the Authorization Server's local database, and, if needed, authentication of the user to the user's trusted identity provider, the Authorization Server may issue an access token or UMA RPT based on the user's identity as expressed in the token, even if the user has not previously registered with the Authorization Server. Due to the federation of the trust model, each user and each CTS does not need to independently register with each Authorization Server. Further, because identity is federated, a grant can be given authority of "any provider" and have meaning at any Authorization Server.

The advantage to this approach, as opposed to having a CTS for every Authorization Server and a registration process at every Resource Server for every user and every app client, is the ability to associate a patient's identity as data owner with the identities of their grantees, and for this association to persist across multiple health systems. It is also helpful to be able to use profile information from the extended OpenID data in granting entitlements from and to the correct identities. A given identity may include a list of data resources "owned" by that identity, for which access can be granted to others, as well as resources for which access has been granted "to" this identity by another data resource owner.

There are also clear advantages over deployment frameworks that isolate user identity and grants to the context of a single resource server, resulting in repeated user registration (at each resource they wish to access), corresponding repeated grant entitlement assignment for data owners, repeated identity verification for each user (in the context of every data owner or grantee on each Authorization Server), and isolated silos of grant information. Federating the storage of grant data instead allows for universal identity assurances such that identity events do not need to be repeated in the context of each different resource server, which may come to number in the hundreds of thousands nationwide. Additionally, the ability to securely share some profile information or even make public some profile information for directory-like discovery will help in finding patient records themselves and in confirming the right resources are made available to the right person and the appropriate identity is granted an entitlement. Hybrid models are also possible in this scenario, but with the framework to federate identity information, data ownership and grants, the potential for a true consolidated patient record that can be viewed within a single application, by the patient and all representatives, caregivers, and providers requiring access to it, is more efficiently achieved.

Example

Consider the case in which my primary care provider allows me to access my record through her EMR's public API. I register myself for a username and through a mechanism approved by my provider associate this username with my identity to access my records at her practice. I would like to authorize my friend Samantha to access these records as well. In the proposed framework, I can find Samantha's username (perhaps one or more of them) by searching using her known username or her email address that is already known to me. Federated identity services based on verified email addresses would return a list of all discoverable users with Samantha's email as a confirmed email address. I can contact Samantha directly to ask her which identity is preferred if there is more than one result, such as the case where Samantha has previously registered with more than one identity provider. I can select one or more of those usernames to grant access to my records at this provider, to other providers I've linked to my username, or even to all of my providers. I can also limit this grant to one or more data categories, in case I only want to authorize Samantha to some of my data such as my immunizations.

Metrics

Potential metrics for success include the number of Health IT vendors integrating HealthToGo, the number of patients registered through us or a federated partner, the number of UMA RPTs issued by our Authorization Server, or the number of patients who activate UMA-based protection of their healthcare data through our service.

Risks

Unintended data exposure of PHI is the primary concern in deploying this type of project. Our established methodologies for developing and deploying secure infrastructure, along with use of the secure protocols required to allow only authorized access, encryption of data at rest and in transit, and use of cryptographic keys to establish federated identity (when useful to do so), will allow us to execute successfully on this project.

Additional Resources

Please refer to the accompanying slides for mock-ups of the functionality we are proposing.