NSTIC in Health Care

Patient ID Service - Leveraging the Identity Ecosystem to Improve Health Care

Submitted by: Daniel A. Combs, CEO, eCitizen Foundation

Summary

This proposal focuses on meeting needs and filling gaps that will otherwise not be covered or provided by businesses supplying the market or by other organizations participating in either the healthcare or the identity communities. The Patient ID Service, PIDS, is a collaborative effort led by the eCitizen Foundation (a member group of IDCommons) and the Kantara Initiative's Healthcare Identity Assurance Workgroup and involving numerous participating organizations and individuals. The overall effort is built on the foundation of an architecture for patient managed authentication along with implementations based on this architecture that provide patients with capabilities to manage various credentials and identifiers, protect their personal information and perform an active role in their own healthcare. This foundation is the basis for addressing a variety of issues arising in the nexus between the healthcare and identity communities and their operations. This is accomplished by working with various business, government and other organizations and individuals within both communities to develop relationships, facilitate collaboration, foster standards adoption and development, support market development and provide solutions to meet shared needs. The PIDS effort is intended to leverage existing business, legal and technical solutions; identify gaps; and to promote efforts to provide solutions to fill these gaps. This proposal, leveraging the ongoing PIDS effort, includes implementation of a novel approach to bridging the gap between legacy systems without effective authentication (such as patient health records systems, EHR/PHR) with a new and open approach to identity functions that can span multiple health networks. The work under this proposal will involve collaboration with other existing related efforts and will deliver value for the NSTIC effort well beyond the funding requested under this proposal.

Background

Healthcare is the single biggest sector of the U.S., consuming about 18% of GDP. Almost everyone participates in some way. Healthcare, while often an adopter of highly innovative advanced technology, has largely avoided or lagged behind the information technology (IT) revolution. During the upcoming three years, the U.S. government will spend tens of billions of dollars to incentivize adoption of information technology, in particular the use of electronic health records, and billions more will be spent across the healthcare sector in implementations. One key set of functions for providers to obtain these incentives is the capability to provide patient access to their electronic health records. Other programs will develop health information exchanges, health insurance exchanges and other advancements all of which will at some point require a capability to authenticate individuals.

The U.S. General Services Administration in 2005 collaborated with HIMSS to develop a white paper on authentication in healthcare. (See text box.) The Markle Foundation, http://www.markle.org/, which created the Health Consumer Authentication component of their Common Framework, http://www.markle.org/health/markle-common-framework/connecting-consumers/ct2, claims patient authentication is, "A Critical Problem of the Digital Age." Originally, established as a special interest group within the Liberty Alliance Project, the Kantara Initiative's Healthcare Identity Assurance Work Group (HIAWG), has developed a body of work on authentication in healthcare. Each of these efforts,

> The GSA approached HIMSS in 2005 to discuss partnering on a project that would show the applicability of the federally adopted security technology and solutions for healthcare information sharing. (from "HIMSS/GSA National e-Authentication White Paper; http://www.himss.org/content/files/GSAwhitepaper.pdf)

among others, recognized the need for patient identity capabilities. However, the healthcare sector has made limited progress or has postponed taking action to meet these functional needs, and has made even less progress in incorporating the existing tools and techniques of Identity and authentication such as those contained within the NSTIC and developed by its participants. This is now changing as the pressure to rapidly transition to electronic health records is accelerating the need for patient identification and authentication. There is now a unique opportunity to influence this development.

The leadership of both the eCitizen Foundation (eCF) and the HIAWG have collaborated since 2005 to promote, support and develop the ecosystem for healthcare participant authentication and within these organizations have worked together for over two years to develop the Patient ID Service (PIDS), an open architectural approach to providing patient identification and authentication. Initial research and design has been completed and the results are available at http://design.patientidservice.us/. Since the development of the NSTIC it has been adopted as a specific goal for PIDS to be aligned with the Strategy.

The PIDS effort will deliver a common approach to providing patients with the tools to undertake a more integral and active role in their own healthcare by developing the business, legal and technical solutions to manage the various credentials they may hold and resolving a variety of issues related to this capability. This will be accomplished by developing the capability for a patient to manage existing credentials and identifiers for use as standards-based, federated credentials that meet the requirements for interoperability at defined levels of assurance. Implementations based upon the PIDS architecture are intended to be incorporated into various other systems with which patients interact such as patient portals, health information exchanges and benefit exchanges, and electronic health record systems for example.

NSTIC in Healthcare-the Proposal

The focus of this proposal will be to undertake particular efforts that will provide significant value for the NSTIC program and will have an important impact in healthcare. The work included in this proposal is unlikely to occur without the financial support of this program. They are for the most part not central to the organizational interests of participants, but rather are of broad and significant societal value. These efforts will help to introduce and incorporate the Strategy into the healthcare community by leveraging prior and ongoing work and existing relationships. Included in this proposal will be an initial implementation of particular components based upon the PIDS architecture; the conduct of a pilot using those components; and the study, documentation, and demonstration of the specific utility of the pilot for patients and healthcare practitioners. The output of this work will be a combination of software components, documentation, lessons learned, and study results that will either provide or lead to solutions to key issues impeding the adoption of NSTIC in healthcare. All of this will be done under an “open” approach. The resulting documentation and software components will be published under an open license for public use, as is the prior work. The following will be included in the final proposal.

- ***PIDS Patient-centric Credential Management Components***

Patients will be provided tools to manage their credentials, protect and track use of their personal information, and adopt a significant active role in their own healthcare. The first set of tasks will be to implement PIDS functional components such as those for registration and credential management. Existing software will be used where available. This software will be developed as components intended to be incorporated into other patient interface systems. The components under this proposal will include patient registration; registration or creation of an OpenID that will serve as a universal unique ID; registration and binding of other credentials and identifiers currently in use; patient control for privacy and permissions; limited trust elevation to meet anticipated future requirements; and standards or best practices-based authentication and assertions. For the purpose of the Patient-Provider Pilot included below these PIDS components will be incorporated into a Health Information Exchange implementation.

The design and development of these components will provide standards-based, federated authentication by leveraging existing processes, technology and business arrangements. Additionally, this approach will provide an easier migration path for various credential and identity service providers to become standards compliant and for relying parties to adopt the use of standards compliant services through incorporation of these capabilities.

- ***Patient ID Proofing and Patient Data Matching interoperation***

The Healthcare sector addresses patients, as relates to their information, as entities or objects to be managed or as data elements of records, generally not as users. The means to discover patient records, for example in the Nationwide Health Information Network as conceived by the Office of the National Coordinator of Health IT, is based on a technique often called patient data matching (PDM). Incorporating into healthcare operations and practice the tools and techniques developed by identity management (IDM) practitioners and included in the NSTIC will require a capability to translate and interoperate between the common tools and techniques of identity management and those of patient data matching practice. This proposal will include the establishment of a workgroup on Patient Identification and Authentication that will collaborate with existing organized efforts addressing Patient Data Matching for the purpose of creating an analysis of the issues and solutions to address these issues. The result of this work group will be the development of one or more components to meet the identified functional requirements for interoperation between IDM and PDM. This will deliver a key capability necessary for leveraging the work of existing credential and identity service providers for use in the transactions, such as health record delivery to patients and implementation of accountable care models, anticipated by current developments in healthcare.

- ***HIPAA, HITECH, FIPPS & DURSA– Law and Operating Rules for IDM in Healthcare***

There are a number of laws and rules that may well serve as hurdles or barriers for the conduct of identity management as conceived under the NSTIC, such as the Health Insurance Portability and Accountability Act (HIPAA). This proposal will include work with existing groups, such as the American Bar Association – IDM Task Force, to analyze existing law, rules, and agreements such as HIPAA and DURSA to identify issues relating to the conduct of IDM and incorporation of the NSTIC into healthcare and to develop recommendations and documentation to resolve identified issues.

- ***Patient – Provider Pilot***

Incorporation of the concepts of the NSTIC into healthcare practice will facilitate the improvement of healthcare and related business operations. There are, for example, an estimated 100,000+ deaths and billions of dollars of costs resulting from patient identification errors. There are numerous other inefficiencies, costs, and barriers to effective conduct of healthcare and information exchange due to lack of effective, interoperable identification and authentication of patients. Rural providers and small organizations face further hurdles to the adoption of the capabilities.

This proposal will include a pilot project involving patients, healthcare providers, and one or more Health Information Exchanges that will use the capabilities developed under this proposal including a small variety of credentials to improve the practice of healthcare. The pilot will address issues of patient registration, management of credentials, use of credentials and patient authentication in the conduct of healthcare activities and will address issues faced by rural providers and their organizations. The pilot will provide the capability to reduce patient misidentification and facilitate the attainment of Meaningful Use requirements and other secure patient communications and interactions by providers. It is intended that participants in this pilot will include the USPS, one or more State credential issuers, and an existing health information exchange.

- ***Education and Demonstration of NSTIC in Healthcare***

Various healthcare organizations are beginning to address issues of patient identification and authentication. Many have little knowledge or understanding of the work done elsewhere in identity management and incorporated into the NSTIC. This proposal will include the presentation of the documentation and solutions developed for the purpose of demonstrating the value of the NSTIC and educating participants about the Strategy and related solutions. For example, HIMSS holds an annual conference in late winter. The conference attracts more than 30,000 healthcare decision makers, practitioners and interested parties. There will be developed a demonstration version of the PIDS components and this demonstration will be presented at the HIMSS conference among other venues. Online educational material and the documentation for the project will be available and promoted for community use.