

Introduction

SAFE-BioPharma Association is grateful for the opportunity to review and comment on ONC’s draft, “A Shared Nationwide Interoperability Roadmap.” SAFE-BioPharma was created by the biopharmaceutical industry and its regulators to provide global high-assurance identity trust for cyber-transactions across the biopharmaceutical and healthcare sectors. SAFE-BioPharma is the only industry collaborative that operates two trust federations approved by the U.S. Federal Identity, Credential and Access Management (FICAM) subcommittee of the US CIO Council and that includes high assurance authentication and digital signing services recognized by the European Union and the European Telecommunications Standards Institute Qualified Certificate Program.

SAFE-BioPharma believes that one of the fundamental requirements for national healthcare interoperability is standardized identity trust. It provides a tool for firms, vendors, regulators and others to standardize trust for authentication and signing. It allows industry, government, vendors and individuals to know that their products or the products/applications they are using are acceptable across the healthcare landscape and can be confidently used by all stakeholders.

Further, standardized identity trust allows users to have only one on-line identity for use with all partners, should they so choose.

General Comments

The SAFE-BioPharma Association believes that one of the most powerful steps that ONC can take to protect the privacy, security and confidentiality of medical data is to recognize the critical need for high assurance of identity for all entities that touch the Health IT architecture. This includes identity for devices, for government, for business entities and for individual practitioners and providers. Devices communicating with the Health IT architecture must assert identities as reliably as persons. The FDA is currently developing a program to confidently identify Internet-connected medical devices and we recommend that this initiative be folded into Roadmap design and planning.

We also believe that all assertions of identity within the Health IT architecture should conform to NIST standards and guidelines for cybersecurity and online identity assertion and the US FICAM policies regarding trustworthiness of identity assertions based on those guidelines. While we also believe that **“one size does not fit all,” we believe that there must be a minimum baseline “size,” which replaces all single factor userID/password authentication implementations with two-factor authentication implementations.**

As technology advances more rapidly than government policymaking, it is important to understand that standards, guidelines and policies are based upon the principle of identifying risks and developing adequate mitigation strategies to counteract them. There are many ways to implement use case appropriate two-factor authentication implementations that satisfy NIST standards and guidelines. One example might be for the identity assurance of a low-assurance, single factor identity credential such as userID/password to be improved when the relying party employs a second factor test at time of login, as



is currently done at many online banking sites. This aligns well with industry, technology and societal migration to universal connectivity and mobile device proliferation. A stronger, two-factor credential would be more appropriately required for a systems administrator to log in to a critical, PHI-filled data repository. Requirement of such a credential likely would have saved Anthem from the hacking disaster it recently experienced.

For privacy, security and regulatory compliance reasons, we reiterate that all sensitive data be encrypted at rest and in motion with asymmetric key cryptography conformant with NIST standards and guidelines and with the guidelines of the CA Browser Forum. In order to ensure broad interoperability and trust, all device, individual and organizational digital certificates for high assurance of identity should be issued and managed by services cross-certified with the US Federal PKI Architecture directly or indirectly.

Assured identity management is one of the three foundations of cybersecurity identified in the President's Report on cybersecurity issued in 2009. The Interoperability Roadmap rests upon the assumption of broad sharing and collaboration and it must therefore include a substantive, yet flexible, identity management component. We support the Roadmap's position in its section on "Verifiable Identity and Authentication of All Participants" while recommending a more nuanced requirement for minimum two-factor authentication based on risk and risk mitigation as a design principle.

Specific Actions

SAFE-BioPharma Association would welcome the opportunity to share its expertise in support of ONC efforts to focus on implementation of identity assurance and the important part that interoperability contributes as part of any overall cybersecurity initiative.

Mollie Shields-Uehling
President and CEO
The SAFE-BioPharma Association
Mollie@SAFE-BioPharma.org
201 925-2173
www.SAFE-BioPharma.org