LSCP Life Sciences
Consulting Partners

The LSCP eHealth Dossier

Interoperable
Digital Identity Management in the
Electronic Exchange of Health Information

An Expert Panel Report

The Executive Summary

December 17, 2007

By courtesy of

SAFE-BioPharma™

SAFE-BioPharma Association

With support from:

eHEALTH INITIATIVE
Real Solutions, Better Health

Process and Acknowledgements

This report was written with input from a panel of experts from both health information exchange (HIE) initiatives and digital identity management from the biopharmaceutical, defense and financial services industries, as well as the federal government. The successes in these three industries and the public sector in developing cross-industry trust and identity management processes have helped guide the recommendations for implementing solutions for HIEs in the future. HIE panelists provided invaluable review and practical input that is vital to the implementation of digital identity management solutions within a health information exchange environment. The participation and input of all expert panelists is greatly appreciated.

Members of the expert panel included:

Holt Anderson, North Carolina Healthcare Information and Communications Alliance, Inc.
Nancy Archer, Arkansas Foundation for Medical Care
Mike Berry, HLN Consulting, LLC; Vermont Information Technology Leaders
Malcolm Bertoni, Food and Drug Administration
Carol Bickford, American Nurses Association
Laura Bowser, Gemini Security
Kirk Brafford, Maximus
Kay Bross, Procter & Gamble Company
Rodney Cain, HealthBridge
Vicki Estrin, Vanderbilt Center for Better Health
Jim Hansen, CareEntrust
Peter Hesse, Gemini Security
Al Jackson, RxHub
Joy Jacobsen, CareEntrust
Marc Lassaux, Quality Health Network
Alex Low, United Hospital Fund
Tim Morris, Centers for Disease Control and Prevention
Charles Parker, Masspro
Daniel Pfeifle, Exostar
Eileen Poland, AstraZeneca
Lori Reed-Fourquet, e-HealthSign LLC
Randy Sabett, Sonnenchein Nath & Rosenthal LLP
Gary Secrest, Johnson & Johnson
Mollie Shields-Uehling, SAFE-BioPharma Association
Toby Slusher, Centers for Disease Control and Prevention
Dick Thompson, Quality Health Network
Richard Thoreson, U.S. Department of Health and Human Services
Rich Ware, AstraZeneca
Karen Wendel, IdenTrust
Monroe Wesley, Vanderbilt Center for Better Health
Brian Witt, Arkansas Foundation for Medical Care

Special thanks to Rich Furr, SAFE-BioPharma Association and to Christine Bechtel, Andrew Weniger and Aaron Holman of the eHealth Initiative who supported and conducted research and worked with the many contributors in drafting, editing and completing this paper.

Executive Summary

The American healthcare system is beginning to recognize the necessity for a reduction in reliance on antiquated paper-based systems and is in the midst of transforming to an interoperable, secure and reliable electronic system. As individual clinicians, hospitals and other care-providing facilities begin to undergo this transformation, new opportunities and challenges arise continually, including in the area of security and identity management.

Secure electronic health information exchange (HIE) across the country is reaching a point which necessitates effective, efficient identity management solutions to address the myriad legal and logistical issues that impact secure, rapid and reliable health data exchange. Other industries have faced this problem in the past and have implemented solutions which may be applicable to an HIE environment. This paper examines factors intrinsically related to identity management in HIE as it relates to clinicians and healthcare providers. While much work remains to be done in the areas of patient identity management and consent to share information, this paper focuses on identity management processes and issues as they relates to care providers in a health information exchange initiative, and draws from what other industries and the federal government have done to address the same issues. The intent of this examination is to provide potential paths forward to address the risks associated with HIE identity management among providers.

Preservation of the security and integrity of health data, while using an interoperable infrastructure, is central to this debate. Wrongful disclosures of electronic health data can be disastrous for both providers and patients. Yet clinicians need access to health data quickly and easily in order to provide care safely and effectively. Therefore, it is necessary for identity management systems to address issues of authentication, authorization, access and audit control. These are the four key cornerstones to any system of trust in a digital environment. How does a system prove someone is who they say they are? If that person is who they say they are, how does a system know what that person should or should not be able to see and do? Beyond these, how does a system track who has seen and done what, and when? The answers to these questions build the basis of trust that is, and will be, needed to support the electronic transfer of health information.

A myriad of factors must be considered when attempting to incorporate digital identity management strategies into the electronic exchange of health information. The federal government provides specific guidance related to the management of identity in an electronic paradigm. The basis of all this guidance is **risk.** System owners must assess the risk inherent in the use, and more importantly the misuse, of the data developed, maintained and archived by any given system. The greater the risk, the more significant the need to assure users' digital identities are tightly bound to individual users in a manner that can assure relying parties (medical professionals, system administrators, payers, auditors, and most importantly, patients) that the data on those systems is protected from exposure.

There are numerous methods to manage identities, control system authentication and authorization for the use of, and access to, specific information and the audit and accounting of who accessed information, when and what did they do with it. These range from simple and rudimentary identity management based on virtually no verifiable information, to much more tightly controlled personal identity verification schema implemented in scenarios in which the risk to data from a number of perspectives is high. After identities have been verified, with the appropriate level of scrutiny, authentication to systems is also possible using an array of methods, again from the simple and relatively insecure to the highly secure and controlled.

Cost and technical complexity were historically the primary barriers for many organizations participating or contemplating participating in exchange. The technology to implement strong identity management has evolved rapidly and the costs have shrunk significantly over the past few years to the point that individual practitioners and almost any HIE can afford implementation. Concomitantly, the technical complexity surrounding public key infrastructure (PKI), arguably the most secure means to manage identities, has also been reduced significantly.

The healthcare industry is unique in a number of ways. Many care providers and facility managers who need access to critical health information are not as easily linked to a single employing entity as say, a scientist in the biopharmaceutical industry. In an environment in which individual clinicians may potentially work for many different care facilities, the need for an identity that transcends regional and employment proximity is necessary. This need also presents a difficult, but not insoluble, problem in developing trust and recognition between facilities. If a nurse or physician, who performs a specific role - for example emergency room staff - works part time at two separate health facilities, are their credentials tied directly to them as an employee of a specific institution, to them as an individual or to them as a subscriber to a larger system of trust? The use of digital identity certificates and federated identity systems provides the means to assure this professional can use their credentials in multiple environments to access the data they require to provide the best quality care at any given time.

A second factor to consider when investigating identity management is the effect on workflow disruption. If a single or two factor authentication process is necessary for a clinician to access health data, that authentication process must readily scale to cover all relevant processes with which the clinician interfaces during the course of a normal day. If not, clinician resistance may be strong, time will be wasted, a care facility's resources needlessly squandered and, most critically, patients may not be afforded the level of care they deserve. The need to confront these issues and provide a single digital identity that quickly and securely interfaces with multiple infrastructures and systems at multiple levels is critical. The ability of systems and infrastructures to support single sign-on will help resolve these issues.

There are a number of systems currently in use in healthcare that provide for authentication and authorization to access health data. How many of these systems interoperate smoothly? HIPAA regulations provide us with a number of structural and legal steps that any care facility must consider when dealing with health data. Many states have also passed and implemented legislation that requires even tighter controls than HIPAA. Illegal disclosures or unauthorized breeches of these sets of data can be costly, and more importantly, they can dramatically set back efforts to mobilize health information to improve patient care. Thus, there is an underlying requirement for system integrity and security that is inherent to the concept of health information exchange. If one facility believes its data systems to be HIPAA compliant and meet other stringent security policies, but is unable to trust that a neighboring facility has afforded the same scrutiny to its systems and policies, that mistrust will reduce the likelihood of effective data exchange. Although this may mitigate legal risk, it does not contribute to the many enhancements technology can bring to healthcare in today's world. While interoperability on a data sharing level is crucial, the ability to build trust in the identity of authenticating users is also critical. Without a common means to assure identity and thereby control authentication and access, the ability to exchange data will be severely limited.

The real benefits accrue as the web of trust expands outward from one organization to encompass the multiple organizations participating in even one HIE. With the malleability of digital media, most authors on the subject state that digitally signed assertions of identity will become the standard.

For most applications that require strong authentication, PKI-based authentication provides the most secure means to meet all requirements. Recent advances in Public Key Infrastructure (PKI) technology provide scalable, reasonably priced options to manage identities in a manner that strongly ties a digital identity, based on a cryptographic certificate, directly to a specific user. Such capability provides relying parties assurance that the person on the other end of the transaction is truly who they purport to be.

Other industries have faced these challenges and opportunities before, particularly in the banking, biopharmaceutical, defense and public sectors. As a result of a review of relevant experience, processes and procedures in these sectors, this paper finds the following:

Recommendations and Findings:

Findings

- HIE has the potential to significantly improve the quality of healthcare, and therefore the health, of the American populace;

- HIE, to be truly successful, requires the application of consistent standards and policies that can work in harmony across state boundaries, including policies for digital identity management;
- Technology continues to evolve, both in identity management and data systems interoperability. As these technologies evolve, health information exchange initiatives will have to maintain awareness of this evolution and can take advantage of these advances.
- Digital identities that are tightly bound to the individual provider offer significant benefits, especially in terms of trust assurance and security, in processes involving authentication to systems outside of a user's parent organization;
- The development of a nationwide network of trust, predicated on strong identity management, is critical to moving HIE forward;
- There are existing models for the development of networks of trust that bear understanding and either implementation or modification to meet HIE needs. It is not necessary to reinvent the wheel.

Recommendations

General Recommendations:

- Awareness of identity management and the need for standard policies and interoperability should be expanded across national public and private sector initiatives, as well as the HIE community;
- Policies and procedures for identity management in HIEs should be further explored and tested in 2008, and lessons learned should be reported to the HIE community.
- To support and foster interoperability, the rules implemented as part of the Federal Common Policy should inform the identity management policies of HIEs.

Members of the SAFE-Biopharma community make the following specific recommendations to HIEs. These recommendations are based on their experience in exchanging sensitive clinical research and other proprietary data between companies, regulators, clinicians and others:

- Form trust networks through a system of closed contracts. The use of a closed contract model provides safeguards by removing enforcement from state or other jurisdictional law, and places it under contract law. It binds members to approved policies and procedures, allows arbitrated dispute resolution, provides the ability to set liability limits and eliminates cumbersome bilateral agreements. This will help address potential issues when HIEs begin to interact with other HIEs as part of a nationwide health information network (NHIN) and provides a common set of policies and guidelines for identity management.
- Develop common policies, procedures and guidelines in order to bind users to them through contracts. The common policies and guidelines developed in closed contract models provide a standard method to manage the life cycle of a digital identity, with specific responsibilities levied on actors in the system at various points. This provides the means to enforce specific actions and consequences for failure to adhere to the rule set. It also provides clear and unequivocal guidelines to all actors for the use of digital identities managed within the system.
- Separate authentication and authorization. Authentication confirms, asserts and validates an identity as being the individual, while authorization grants specific rights based on authenticated identity.
- Authenticate as an individual (vs. organization or role), and authorize based on role. There are a number of ways to implement this recommendation that should be investigated. Roles in digital certificates may present issues in the life cycle management of such credentials that impact the users, especially if their role changes.
- Consider cross-certification with Federal Bridge CA as part of the architecture for NHIN identity management. This would provide interoperability with federal agencies, and potentially provide a platform for use by all networks participating in the NHIN.