ITL BULLETIN FOR NOVEMBER 2010

THE EXCHANGE OF HEALTH INFORMATION: DESIGNING A SECURITY ARCHITECTURE TO PROVIDE INFORMATION SECURITY AND PRIVACY

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Improved, more effective healthcare is a high priority in the United States today. While the U.S. healthcare system is widely recognized as one of the most clinically advanced in the world, costs continue to rise, and often preventable medical errors occur. Government and private sectors are collaborating to improve the healthcare infrastructure and to facilitate the secure exchange of electronic health information through electronic health records (EHRs). These efforts are expected to lead to better patient care, fewer medical errors, and reduced costs of healthcare in the United States.

Health information technology (HIT), especially the development of electronic health records for use in both inpatient and ambulatory care settings, has the potential for providing reliable access to health information. Currently, health information is scattered among healthcare providers and payers. Patients have limited control over the collection, access, use, and disclosure of their health information.

The goal of storing, moving, and sharing health information in electronic formats raises new challenges for ensuring that the data is adequately protected. Better management of electronic health information will depend upon its secure exchange between consumers, providers, and other healthcare organizations in ways that safeguard the confidentiality, integrity, and availability of the information.

The sharing of healthcare information can take place in many ways, including through health information exchanges (HIEs). HIEs can involve exchanges between two organizations in a community, or between several organizations in a region, in several regions, or nationwide. Exchanging organizations need a structured approach to security, which will enable their information systems to protect health information before, during, and after the exchange. All aspects of data usage, including collection, storage, modification, and destruction, will require security and privacy protection.

Government and commercial organizations already use widely accepted practices for protecting their information and information systems, and these practices can be applied to the health information exchange process. This approach involves addressing the protection of health information throughout the system development life cycle, and applying protective mechanisms, including contingency and disaster recovery planning, configuration management, and other processes and technologies, to the secure exchange of health information.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST), which has been collaborating with industry and others to improve the healthcare information infrastructure since the 1990s, recently published a new guide to assist organizations in developing a secure architecture to provide for the security and privacy of health information.

NIST Interagency Report (NISTIR) 7497*, Security Architecture Design Process for Health Information Exchanges (HIEs)*

NISTIR 7497, *Security Architecture Design Process for Health Information Exchanges (HIEs)*, describes a systematic approach to designing a technical security architecture for the exchange of health information by building on common government and commercial practices, and demonstrating how these practices can be applied to the development of HIEs. Written by Matthew Scholl and Kevin Stine of NIST and by Kenneth Lin and Daniel Steinberg of Booz Allen Hamilton, the publication assists organizations in ensuring that data protection is adequately addressed throughout the system development life cycle, and that data protection mechanisms are applied when the organization develops systems for the exchange of health information.

The report describes the scope and characteristics of four HIE contexts: Ad Hoc, Regional, Multi-Regional, and Nationwide. These contexts are the conditions under which the information is transmitted. The guide focuses on the development of Regional HIEs.

One section of the report presents the HIE architecture design process and introduces the five-layer operating model that can be used for designing a security architecture to support the exchange of health information. Systems for the exchange of health information involve different business functions and technical layers in order to address complex data protection issues.

The security architecture process applies to the exchange of health information and the deployment of HIEs. The architecture can be used to protect health information at various risk and sensitivity levels. This process, for example, can accommodate high-risk health information, such as information about treatments provided to particular patients, as well as lower-risk information, such as information that may be publicly available through other means, yet remains sensitive when available in combination.

Other topics covered in the publication include detailed descriptions of the five-layers that compose the operating model, and the process for building a nationwide HIE using regional HIEs and federated security services.

The appendices include an example of the security architecture design process as applied to a specific American Health Information Community (AHIC) use case to illustrate the analyses and considerations needed when applying the process to the exchange of health information. The detailed, multistep scenario that is presented considers issues and data

flows surrounding the implementation of information technology to enable the delivery of personalized healthcare. Charts, tables, and illustrations help to explain the process. The appendices also provide definitions of acronyms used, a glossary defining the terms used, and references and related source material.

Health Information Exchange (HIE) Contexts

There are many conditions under which health information can be exchanged. Information can be sent to and from many different kinds of entities, in various forms of media, and can be subject to a wide range of laws, regulations, and policies. The four main HIE contexts discussed in this publication are:

• An **Ad Hoc** HIE involves two healthcare organizations exchanging health information, usually under the precondition of familiarity and trust, using existing and usual office infrastructure such as mail, fax, e-mail, and telephone calls. Health organizations that currently participate in Ad Hoc HIEs may find it impractical to justify the cost of migrating from these activities to EHR-based HIEs unless there are specific incentives to make the process more appealing, or regional resources are available to make the process easier. An Ad Hoc HIE can be effective for small-scale exchanges of health information, but Ad Hoc HIEs may not be able to integrate easily with each other in order to grow and expand. This growth requires familiarity with the participants and technologies used to create the infrastructure. Without sufficient trust in the resulting larger HIE and its participants, members of the Ad Hoc HIE may be reluctant to place the privacy and security of their own information and systems at risk.

• **Regional** HIEs consist of two or more legally and commercially independent institutions that share EHRs, when there are no state jurisdictional issues that prevent or impede the sharing of data. The HIE network includes clinicians, hospitals, laboratories, pharmacies, insurance companies, and other key health domain players. Participating organizations will normally draft a trust agreement to govern the information exchange. Depending on the scale, the technical architecture might be centralized or federated. Regional HIEs are large enough to justify the associated operational costs because the efficiencies realized offset the costs. They are simpler to administer than Multi-Regional and Nationwide HIEs because of their smaller scale and lack of state jurisdictional conflicts.

• **Multi-Regional** HIEs connect multiple Regional HIEs and may exist across state lines or other physical boundaries. They are usually EHR-based. Since they connect multiple Regional HIEs, they are likely to have a federated technical architecture. For Multi-Regional HIEs, conflicts of laws may require complex solutions.

• A **Nationwide** HIE would connect many Regional or Multi-Regional HIEs. It would require the use of some form of EHR, involve multiple state jurisdictions, and have a nationwide federated technical architecture. Multi-Regional and Nationwide HIEs have a different focus than Regional HIEs. Regional HIEs are basic building blocks that focus on developing effective and localized solutions to meet specific HIE needs, such as

research, clinical trials, and patient transfer. Multi-Regional and Nationwide HIEs focus on building the backbone infrastructure needed to connect the various Regional HIEs.

The guide concentrates on the development of **Regional HIEs**. If the security architectures and other system aspects of Regional HIEs are interoperable, these HIEs can then serve as building blocks for larger **Multi-Regional HIEs**, and eventually can be the basis for a broader, scalable solution, leading to the future development of a **Nationwide HIE**.

The Five-Layer Security Architecture and Design Process

Technical solutions that facilitate the exchange of health information can be complex. With various policies and standards, and an ever-changing technical landscape to be considered, a systematic approach to designing an HIE security architecture can allow practitioners to analyze all policy requirements and to refine them into a technology-neutral, vendor-neutral, standards-based architecture to drive technical solution decisions. The use of a systematic approach plays a significant role in a successful and secure HIE implementation.

The HIE security architecture design process assists HIEs in meeting this need by providing a five-layer methodology for the identification and selection of the HIE security technology needed to protect health information. The five layers, or phases of activity, are:

• **Layer 1, Capstone Policies**, which are developed by an organization to incorporate all requirements and guidance for protecting health information within HIEs. The contents and scope of Capstone Policies can be driven by state or federal laws or regulations, organizational policies, business needs, or policies developed for specific HIEs. The most efficient developer of the Capstone Policies will be the organization that can set standards for the entire HIE. A single participant in an HIE, for example, may be subject to a certain set of laws, but coordination across the entire HIE will be necessary to ensure that all drivers of Capstone Policies for all desired participants are identified and incorporated. A listing of the laws and regulations that may affect the healthcare transactions for some entities is provided in the guide.

• **Layer 2, Enabling Services**, which define the nomenclature of services required to implement Capstone Policies. Enabling Services are designed to be HIE context-independent. Services covered in the guide are derived from common industry-wide data protection practices and then customized to specifically address the requirements of HIEs. A consistent, standards-based set of Enabling Services can benefit future interoperability among HIEs. This standardization provides a basic assurance level on the implementation of security and privacy controls, making it easier to determine and address discrepancies among HIEs. References to legislative and regulatory requirements and to NIST guidance are provided.

• **Layer 3, Enabling Processes**, which define the operational baseline with use cases and scenarios for Enabling Services. Enabling Processes are HIE context-dependent and define business processes for Enabling Services. While Enabling Services are a platform for an HIE's data protection requirements, Enabling Processes expand the Enabling Services into detailed requirements, usually in the form of use cases or scenarios, based on an HIE's business practices. HIEs of different contexts could implement the same Enabling Services with different Enabling Processes.

• **Layer 4, Notional Architectures**, which define the major technical constructs, such as role-based access control and directory services, and their relationships to implement Enabling Processes. The Notional Architecture is the blueprint to drive the selection of technical solutions and data standards. The Notional Architecture is standards-based, technology-neutral, and vendor-neutral. It is dependent on the Enabling Processes and will vary between HIE implementations. In addition to the inputs from the Capstone Policies, Enabling Services, and Enabling Processes, the Notional Architecture must consider architectural design principles, which are derived from the experiences of organizations that have implemented information-sharing networks, and architecture constructs, or design structures, that can serve as the basic building blocks for a Notional Architecture.

• **Layer 5, Technology Solutions and Standards**, which represent the selected technical solutions and data standards needed to implement the Notional Architecture.

The security architecture design process that is described in the publication provides a scalable, standardized, and repeatable methodology to guide HIE system development in the integration of data protection mechanisms across each layer, and results in a technology selection and design that satisfies high-level requirements and mitigates identified risks to organizational risk tolerances. The architectural design process allows for the integration of nontechnical issues such as those related to laws, regulations, and policies, specific roles and responsibilities, training, human resources issues, or nontechnical privacy issues, into the information technology architecture of an HIE.

Protecting Information Security and Privacy

NIST has been working with federal, state, and local government agencies, industry groups, standards organizations, and others in the healthcare community to improve the healthcare infrastructure. NIST focuses on the tools, technologies, and methodologies that advance the development and deployment of reliable, usable, interoperable, and secure information and communication systems.

Under the Federal Information Security Management Act (FISMA) of 2002, Title III of the E-Government Act (Public Law 107-347), NIST's Information Technology Laboratory develops standards and guidelines to support federal agencies in protecting their information and information technology systems.

Other legislative mandates affecting federal information security requirements include the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191). HIPAA requires the Secretary of Health and Human Services (HSS) to adopt, among other standards, security standards for certain health information. These standards are known as the HIPAA Security Rule.

Related Activities

NIST is working with government, private sector, and voluntary standards organizations including Health Level Seven (HL7), the Institute of Electrical and Electronics Engineers (IEEE), the International Organization for Standardization (ISO), and Integrating the Healthcare Enterprise, to identify current standards that are applicable to healthcare information and to develop new standards that will be needed in the future.

To help implementers of health information technology systems, NIST is developing testing activities, including test tools and associated testing infrastructure, to enable system developers to confirm that their systems meet specifications and can exchange information with other systems. A set of approved procedures for testing information technology systems that work with electronic health records has been published. These test procedures evaluate various components of electronic health records such as how they plot and display growth charts, how they implement encryption, and how they control access so that only authorized users can access health information.

NIST is helping to develop a program for the voluntary certification of health IT systems for compliance with criteria governing performance of specifically defined functions. Testing organizations authorized by the U.S. Department of Health and Human Services Office of the National Coordinator (HHS/ONC) will use the test tools to evaluate EHR software and systems that vendors would like to sell to doctor's offices, hospitals, and other healthcare providers.

See the following Web page for more information: http://healthcare.nist.gov/.

For More Information

NIST Special Publication (SP) 800-66, Revision 1 (October 2008), *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, provides information about the HIPAA Security Rule, including resources for understanding and addressing its requirements. This publication discusses security considerations and resources that may provide value when implementing the requirements of the HIPAA Security Rule, and helps to educate readers about information security concepts and terms used in the HIPAA Security Rule. The publication includes information about NIST resources and publications; discusses the latest threats, vulnerabilities, and exposures, as well as the technologies used to combat those exposures; proposes methodologies for addressing specific Security Rule implementation challenges such as conducting risk assessments and developing

contingency plans; and sets the stage, through security control mappings, for secure automation of the technical safeguards.

NIST SP 800-66, Revision 1, is available at http://csrc.nist.gov/publications/PubsSPs.html.

For a discussion on the HIPAA Privacy Rule, see materials available through the HHS Office of Civil Rights at http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html.

NISTIR 7497 refers to other NIST publications covering the protection of information and information systems. Information about these publications and about NIST's information security activities is available from the Computer Security Resource Center at http://csrc.nist.gov/.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.