Liu, W.; Park, E.K.; Krieger, U.

eHealth Interconnection Infrastructure Challenges and Solutions Overview

Primary publication

Liu, W.; Park, E.K.; Krieger, U. (2012): eHealth Interconnection Infrastructure Challenges and Solutions Overview, in: Proceedings of the IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom), 2012, Beijing, 10-13 Oct. 2012, Piscataway, NJ: IEEE, pp. 255–260, doi: 10.1109/HealthCom.2012.6379417.

eHealth Interconnection Infrastructure Challenges and Solutions Overview

Dr. W. Liu
School of Science and Technology
Georgia Gwinnett College

Dr. E.K. Park
VP for Research and Dean of Graduate Studies
California State University - Chico

Prof. Dr. U. Krieger
Department of Information Systems and Applied Computer Science
Otto-Friedrich University Bamberg

***Abstract*—The research efforts for a national eHealth interconnection infrastructure and design guidelines are in great demand. This paper identifies the major challenges in eHealth interconnection network services that are critical to universal deployment. An overview of our solutions framework is summarized with the aspects of interconnection services, operational management services, and security control services.**

***Index Terms*—** eHealth Interconnection infrastructure, End-to-End Control, eHealth Service Security, eHealth Operations and Service Management, Solutions Overview.

I. Introduction

Digital healthcare solutions will transform the whole healthcare process to become more efficient, less expensive and higher quality [1, 2, 3, 4]. The US government has pledged billions of dollars to help hospitals and clinicians develop and implement systems for digital health records and information sharing [5]. Independently, the industries also gear up developing information sharing technologies [6] within the digital health networks. With additional significant investment by both private and public sectors, we expect that eHealth solutions will soon experience the same advances in other industries (e.g., telecom and banking) when IT systems and networks were deployed in the past.

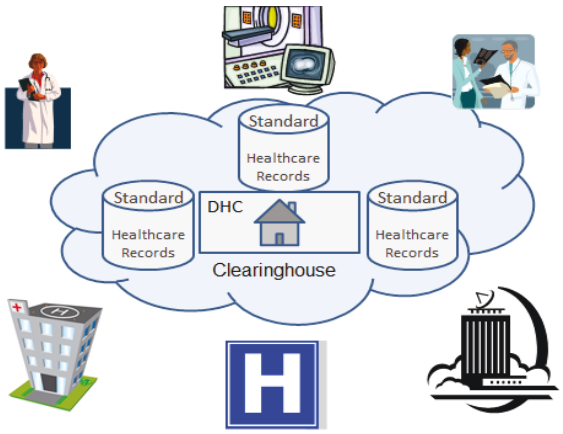

Figure 1. eHealth Interconnection Environment

Figure 1 above depicts an environment that supports access from individual outlets and test facilities as well as insurance providers and government agencies. All rely on a new infrastructure for eHealth.

A successful eHealth implementation has to address a new paradigm in interconnection infrastructure: from proprietary record ownership to networked consumption of health record; from ad-hoc networking to interoperable interconnections; from separated IT solutions to orchestrated service creation and management with quality of service guarantees. All aspects of the new paradigm shall impose new challenges in the underlying consumer network and services infrastructure.

In this paper, we explain the major challenges to the eHealth infrastructure in section II. The emerging solutions are presented in section III for interoperable interconnections, security controls and service level guarantees. And finally, section IV summarizes the key contributions of this paper.

II. Backgrounds and Related Works

A. *System Interconnection Challenges*

In early 2000's, healthcare IT systems are only isolate solutions that did not take the holistic view of healthcare process and outcomes. A number of initiatives have been reported to reform the healthcare IT systems, with a mix of success and failure results [6, 7].

The HITECH (Health Information Technology for Economic and Clinical Health) legislation provided additional monetary incentives to interconnect to the eHealth systems. The major exchange infrastructure enables transmission of electronic health records covering patient demographics, progress notes, medication problems, prescriptions, vital signs, past medical history, immunizations, lab data and radiology reports.

In the NHIN [8] Interconnections example, Internet technology was leveraged to create a network of networks as a way to facilitate secure and interoperable exchange of health information between geographically disparate providers and users of health information. Use of the Nationwide Health Information Network as an infrastructure provides secure transport of existing clinical data from electronic health

records. Additional eHealth gateways may further connection additional digital healthcare solutions.

Other element layers and service layers could be extended from NHIN to ensure service interconnections. These are similar to the examples in [9], where additional operational management functions are added to achieve application level interoperability, including service profiles management, administrative management in monitoring, configuration, performance monitoring, auditing, security management, and service directory for provisioned resources.

The major concern here is to ensure ubiquitous interconnection with the national health information network. The following functions are required to accomplish associations, secure transfer flows, and operations (configuration, security setup, audit tracking and logging etc.). This list is for illustration only, and is not meant to be comprehensive because a complete set must be aggregated and agreed to by a universal standard panel in order to ensure interoperability:

- Association of end-points has to be built upon network connections, but the association does not require dedicated connection channels. The association (sometimes called electronic bonding) authenticates the participating entities which are user or system end points. These aspects of interface requirements are missing (if not entirely) in current national health information network trials.
- The association setup process required provider identification, directory look-up and entity validation, subject data or functional context negotiation. Additional requirements include management of consumer choices not to participate in network services; support of consumer information location requests and data routing to consumer identified personal health records; and arbitration of subject and data identity; as well as other well-known security functions (encryption, integrity validation, and so on). A set of registries can facilitate connections and further association process.

B. eHealth Security Challenges

New security concerns arise in transmitting and processing of electronic medical records, personal healthcare records, patient billing records, as well as public health alerts, among many parties with varying security, privacy and trust levels.

(1) As more and more healthcare providers are expected to convert internal data and transmit digital records over external infrastructure, passing multiple hops, there is a need for security guarantees with end-to-end control. The target rates of electronic healthcare records are 90 percent of doctors and 70 percent of hospitals by the end of this decade [10]. And mandatory reporting on security violation will be imposed and audited.

(2) When digital records can be easily shared, multiple parties are involved in eHealth transactions. While traditional security protocols govern two end-points, a new security paradigm of coordination has to be developed over healthcare network to accommodate diverse users while achieving scalability. Some study [11] estimated as many as 400 people may have access to one's personal medical information throughout the typical care process. Additional government and commercial entities will further tap into the eHealth access infrastructure when electronic records are online. For example [12], even the Social Security Agency is participating in a trial to access electronic health record info for the purpose of determining evidence of disability claims.

(3) At any time, many collaborating providers may possess variable visibility/right of the data. Some parts of the record are confidential patient personal information while other fields are epidemic information for public analysis and research. And still there are other portion of the records such as billing and plan usage information for a few limited parties. A single encrypted data payload can no longer meet everyone's needs. An agile solution has to be found to allow fragmentation in diverse security settings while varying the protection levels at a different processing node. The secure interconnections flows may include the followings.
   - Government Regulated Data Sharing requires to clearly identify the patient by name and demographic information as well as the medical conditions being reported.
   - Insurance Data Sharing requires the hospital to share any diagnostic and treatment information.
   - Connect to Dictation Services may forward notes about the patient so that the information get transcribed for entry into the patient's EMR.
   - Connect to Collection Agencies: A SP can utilize the services of a collection agency in an attempt to recover a portion of the outstanding balance.
   - Supporting Services may include a cloud-based server service for the purpose of scalable server services on-demand.
   - Patient Portal Relationship: A patient portal allows a patient to connect to a portal provider through a secure channel, such as an encrypted feed.

Still another challenge in eHealth security is the efficiency of the solutions. For example, some portion of the patient records may not be relevant to another eHealth party (e.g., such as the Lab processing entity thus only needs a patient identity without the detail records). With multiple parties in secure eHealth association(s), the potential growth of combinations is not scalable.

C. QoS and Operational Challenges

To guarantee Quality of Service in eHealth applications, we need an integrated view to combine 1) the healthcare applications, 2) the interconnection infrastructure support, as well as 3) operational support with common services. Once a holistic understanding of all areas is established, we can better align our research in eHealth interconnection services and end-to-end solutions with QoS guarantee.

The key QoS requirements for the eHealth infrastructure are listed below:

(1) QoS governing Data Communication Components

Vital physiological data (such as body temperature, blood pressure, heart rate and cardiogram and blood sugar level that are constantly monitored by mobile devices) have to be fed into the patient records in real time.

While medical records may not have to be always transmitted in real time, they have to be instantly available during a diagnosis and consultation session with a doctor.

When any change or irregularity happens for a sustained period of time, an alert has to be transmitted within a predefined time interval to the patient and his or her healthcare specialists to enable immediate actions.

A large image or lab report may also impose communication constraints when it is pulled out by a healthcare professional during an e-Health session.

(2) QoS governing e-Health Voice Components

Communication delays should be within a tolerable sub-second session setup time. Delay jitters have to be deterministic in order to avoid misunderstanding of verbal consultations. Medical image displays have to be in synchronization with voice sessions. Unlike traditional networks where voices (real time traffics) are given a higher priority, an e-Health communication channel may coexist with a data session of equal priority.

Any degradation in service level or loss of service can impact the care given to many patients and could delay or hamper a critical surgery.

(3) QoS governing Data Processing Components

A sample implementation may contain the following data processing (interconnection) points that introduced various delays into the message delivery.

- A Database connector (JDBC)
- A (HL7) Low-level Protocol (TCP and under)
- Bulk file exchange connection (FTP)
- Message broker (Transaction Service Bus)
- Message Flow Server connector (SOAP over HTTP or SOAP over JMS)
- Directory search (LDAP)

In addition to the secure interconnection infrastructure, it is essential to provide end-to-end exchange and cooperation of the end users (or message between system end-points). Those interconnection and exchanges have to be augmented with standard operational management messages to implement operational services. Operation and service management is vital to any large scale deployments [13, 14]. There are inherent cost and business responsibilities with maintaining the core services and infrastructure functions (such as protocol versions, measurements, timely cross-system issue resolution or fixes, and continuous performance improvements).

III. SOLUTIONS FRAMEWORK OVERVIEW

A. *Interconnection Infrastructure*

Our solution for e-Health interconnection is illustrated in more details in Figure 2 below, where there are three main layers in our solution framework that consist of the followings functions.

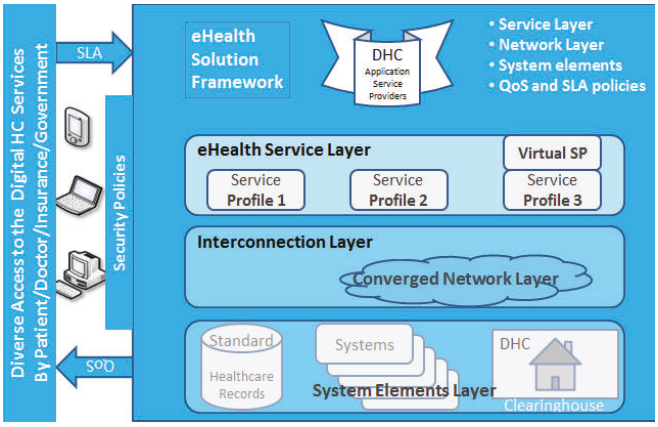

Figure 2. Universal eHealth Interconnection Solution

1) System Element Layer

In the system elements layer, a clinical-support system will gather, store and retrieve patient medical information for use internally by physicians and healthcare workers delivering services at the point of care. The admin and supervisory personnel will have access to backend processing of resources, insurance claims and billings. Other systems support researchers as well as government (e.g., CDC) reporting.

2) Converged Network Layer

A converged network will link the underlying IT element system layer and an eHealth service layer, while allowing pervasive access and ambient applications. The converged network layer also implements interconnections between service providers (e.g., doctor's office to insurance and to lab facilities and so on) via interoperable interfaces.

3) eHealth Service Layer

Finally, the service layer is to present industry standardized service interfaces towards to all partiers served by the digital healthcare infrastructure. eHealth service profiles are used to create, deploy, and maintain policies controlling network QoS which in turn supports patient IT service level guarantees. In addition, the service level agreements between various providers (lab, doctors, pharmacy, and insurance etc.) are all linked to the appropriate profile. In addition to the 3 layers of framework, appropriate backend operation IT systems will enforce the policies and enable the service profile capabilities.

B. *eHealth Security Solutions*

Firms across all business sectors struggle with data security problems and it is unlikely that there is a prescribed solution that will work for all parties handling eHealth records to completely address all aspects of classical security concerns such as confidentiality, integrity and availability. For example, those solutions in the current market usually adopt a point-to-point secure socket transport. And the product level solutions are summarized below:

General Encryption and Decryption of Electronic Health Information	A symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key must be used (e.g., FIPS 197 Advanced Encryption Standard, (AES), Nov 2001).
Encryption and Decryption of e-Health Exchange.	An encrypted and integrity protected link must be implemented (e.g., TLS, IPv6, IPv4 with IPsec).
Record Actions Related to Electronic Health Information (i.e., audit log)	The date, time, patient identification (name or number), and user identification (name or number) must be recorded when electronic health information is created, modified, deleted, or printed. An indication of which action(s) occurred must also be recorded (e.g., modification).
Verification that Electronic Health Information has not been Altered in Transit	A secure hashing algorithm must be used to verify that electronic health information has not been altered in transit. The secure hash algorithm used must be SHA–1 or higher (e.g., Federal Information Processing Standards (FIPS) Publication (PUB) and Secure Hash Standard (SHS) FIPS PUB 180–3).
Cross-Enterprise Authentication	Use of a cross-enterprise secure transaction that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails (e.g., interhealthcare exchange Cross-Enterprise User Assertion XUA with Security Assertion Markup Language SAML identity assertions).
Record Treatment, Payment, and Health Care Operations Disclosures	The date, time, patient identification (name or number), user identification (name or number), and a description of the disclosure must be recorded.
Authentication to control who is connecting.	Accounts/passwords, kerberos, security tokens/IDs, biometrics.
Authorization to control who can access what e-Health information.	Files and DB access control, access control lists; Role/need-limited access: enabling access for personnel only to information essential to the performance of their jobs, and limiting the real or perceived temptation to access information beyond a bona fide need.
Privacy: The right and desire of a person to control the disclosure of personal health information.	Digital signature for controlled release of personal health information to a care provider or information custodian under an agreement that limits the extent and conditions under which that information may be used or released further.
e-Health security perimeters	Firewall and network service management; wireless security protocols. Knowing and controlling the boundaries of trusted access to the information system, both physically and logically.
Information right management	Control information distribution, ensuring that record owners, data stewards, and patients can understand and have effective control over appropriate aspects of information security and access.
Accountability	Helping to ensure that healthcare providers are responsible for their access to and use of information, based on a documented need and right to know. Audit logs are maintained regularly.
Availability	Network and application monitor tools to prevent Denial-Of-Service attacks, ensuring that accurate and up-to-date information is available when needed at appropriate places.

Our design of an end-to-end security solution [1] was to augment the IPsec capabilities with an end-to-end adaptation mechanism to further enhance security control in the eHealth information routing.

In our solution, the end-points agree to what security services are to be offered to the IP traffic, with rules such as types of source/destination (SP, BA, Patient, Portal gateway, etc.), whether it is inbound, outbound, and so on. It contains an ordered list of policy entries, separate ones for inbound and outbound traffics. These entries might specify that some traffic must bypass the adaptive security flow processing, some must be discarded, and the rest must be processed by the implementation modules.

The adaptive secure association process combines the security associations with a service flow scheme. The purpose is to ensure multiple party participations in a controllable way.

- Application Oriented Service Flows – those flows identifying types of eHealth service sessions (provider-provider, provider-insurance, patient-pharmacy, and so on).
- Before communications between two entities in the healthcare exchange, a formal association process is established by transmitting the following information: Entity identifier, roles (sending/receiving), policy restrictions, external/corresponding security manager, and reporting obligations.
- Key exchanges are allowed only if both ends of the Application Ports, or e-Health routing decision points of an eHealth application end-to-end flow, have been formally associated via an adaptation message (containing a persistent security association identifier, key-updates, transaction flows to use the new keys and agreed open policy sets).
- Without the security association process, IP packets are still allowed within the exchanged networks (but without security guarantees). In this mode, existing eHealth over NHIN will be backward compatible with our new eHealth security framework.

Once a secure e-Health association is established, both end points may invite others to participate in the eHealth communication and processing flow. The solution solved the efficiency issue and performance concerns by allowing the parties to have higher-assurance transactions without needing to exchange the details of information that we usually do when registering with a new business online.

- Associating privileges with one or more data components provide the ability to assure that only certain attributes (rather than a complete dataset of personal information) are granted to the right entity:
  e.g., Patient ID credentials (instead of the detail ID#, Name, Address information) are presented from Clinical office to the Lab facilities.
- Sending only the essential (minimum) data that are pre-agreed upon among the e-Health processing parties also enhances interoperable secure associations. Interoperability guarantees anyone using their secure credentials at all sites and ensures that business and other relying parties can accept and rely on certified eHealth credentials.
- This solution encourages service providers to accept a variety of credential and identity media. It also supports identity portability so that patients easily switch providers, thus promoting a competitive eHealth market.

C. *QoS Solutions with End-to-End Control*

1) *Service Profile Management*

Service profiles describe how to implement services for a specific domain or functionality such as bio surveillance or adverse event reporting. The services describe the specific interfaces to be used among interconnection participants to locate and exchange health information.

A few concrete examples of eHealth operational management capabilities include the followings:

- Administrative Management for activity monitoring, configuration, service-level agreement enforcement and performance monitoring, auditing and accounting.
- The Security Service Management capability provides a mechanism for patient permission preferences to be stored and maintained, and thus applied separately from a particular Personal Health Record (PHR) or other mechanism used to enter such preferences.
- Directory provisioning capability allows registration and linkage of entities (care organizations, ancillary result centers, hospitals, etc.) that are directly connected to the healthcare IT infrastructure, allowing those organizations and their systems to be found during queries.
- Configuration management tracks available capabilities and services information for connected users, enabling temporary and permanent de-authorization of direct and third-party users when necessary, and granting emergency access capabilities.
- A performance management function allows threshold reporting, trend analysis and continuous capacity upgrades in order to meet a desired level of service guarantees.

2) *Service Centers*

In our framework, a management center functions are applied to the QoS manager in order to manage the e-Health service and networking.

Operational policies and practices have to be defined for each communication components at the network layer. For examples, it should report delivered vs. contractual Quality of Service (QoS). Failure to meet a contracted SLA may lead to a Service Assurance Warranty payment.

Operational policies and practices will drive the configuration of the (e-Health) service manager. The manager needs to handle end-point performance parameter requests. The manager will also monitor and assist in enforcement of end-to-end transmission performance. Thus, the manager needs access to logs and report functional components.

Control and coordination of the end-to-end network views will be the responsibility of the e-Health QoS manager. The QoS manager can supports Customer Service Management [2, 9] to ensure that a specific e-Health is performing according to specified requirements. It encompasses monitoring the performance, analyzing the root cause of performance problems, and initializing appropriate actions to make sure that classes of service are working efficiently. These processes are responsible for total e-Health service communication quality. The QoS manager may start re-initialization of session once additional communication and processing resources are recovered.

3) *Security Service Manager*

When multiple entities are participating in a coordinated eHealth process, the security associations will be managed by a Security Service Manager to coordinate the communicating groups. An implementation of a security manager shall maintain two databases:

- The Security Policy Database specifies what security services are to be offered to the secure IP traffic [15, 16], with rules such as types of source/destination (Service Providers, Business Associates, Patient, Portal, etc.), whether it is inbound, outbound, and so on. It contains an ordered list of policy entries. These entries might specify that some traffic must bypass the adaptive security flow processing, some must be discarded, and the rest must be processed by the implementation modules.
- The Security Association Database contains parameter information about each eHealth Application Flows, such as eHealth routing algorithms and keys, protocol mode, and flow-level lifetime. For outbound processing, the selective encryption scheme has to be applied. For inbound processing, the Policy Collection is consulted to determine how the packet must be processed. If

necessary, each provider's internal security module is notified to log the processing activities.

Furthermore, the security service managers collaborate with service centers (described in the previous subsection) to guarantee the required functions [8, 17, 18] extended with QoS guidelines.

IV. CONCLUSION

Our research has identified the major challenges in eHealth interconnection infrastructure. We have also documented the security challenges and QoS requirements raised from ubiquitous access of the new digital healthcare functions. Furthermore, we have presented a summary of our solution sets to meet the challenges of new healthcare initiatives with interoperable interconnections, security controls and service level guarantees.

Our research results in a new direction with new distinguished features:

- For the first time, an integrated view (of eHealth application, networking service infrastructure and operational support) is proposed and applied to healthcare pervasive IT applications, in contrast to all existing solutions and without much built-in operational supports. This paper presented the inter-dependence of pervasive healthcare applications, underlying infrastructures and operational supports.
- Our security architecture addressed emerging security needs including universal tracking with ID/certificates, secure associations of entities, multi-party collaborations in "eHealth transactions", and end-to-end security control.
- Our association and service management solutions are modular, letting service providers to build sophisticated identity systems using smaller and simpler subsystems. This implementation philosophy will improve flexibility, reliability, and reuse of these systems and allow for simplicity and efficiency in change management, as service providers can add and remove components as the identity ecosystem evolves.

The approaches as reported in our paper have supplied the much needed guidelines for a leap from digital healthcare trials into the design and implementation of a national level eHealth interconnection infrastructure. Our solutions can accommodate the growth in diverse user community in an interconnected network.

REFERENCES

[1] W. Liu and E.K. Park, "e-Health Security Solution Framework", accepted to appear in 2nd Workshop International Workshop on Privacy, Security and Trust in Mobile and Wireless Systems, August 2012.

[2] W. Liu and E.K. Park, "e-Health Service Characteristics and QoS Guarantee", 1st Workshop on Context-aware QoS Provisioning and Management for Emerging Networks, Applications and Services, Maui, August 2011.

[3] W. Liu and E.K. Park, "Emerging Platform for Healthcare IT Services", IEEE International Conference on Computer Communication Networks 2010, WiMAN Workshop, Zurich, August 2010.

[4] W. Liu, "Digital Health Care (DHC) Information Technology Infrastructure Framework", IEEE Consumer Communications Network Conference, Las Vegas, January 2010.

[5] IT World, http://www.itworld.com/networking/75306/us-pledges-12-billion-digital-health-networks, August 2009.

[6] Jim Adams, IBM Center for Healthcare Management, DHC Keynote Speech: Healthcare 2015 and Healthcare Reform, DHC Conference in Madison, Wisconsin, May 8, 2009.

[7] Mark Ballard, "Accenture: NHS failure is 'track record for success'", Posted in IT Channel, September 28, 2006.

[8] NHIN, "National Health Information Network", U.S. Department of Health & Human Services, http://healthIT.hhs.gov.

[9] E.K. Park and W. Liu, "Wireless Video Services Solution and Management Framework", CCNC 2006, Las Vegas, January 2006.

[10] US Department of HHS, "Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology", January 2010.

[11] S.D. Cannoy and A.F. Salam, "A Framework for Health Care Information Assurance Policy and Compliance", communications of the ACM, vol. 53, no. 3, march 2010.

[12] Feldman, et.al, "Cyber Infrastructure for Secondary Use of EHR Data: SSA's Use of the Nationwide Health Information Network", Proceedings of the 44th Hawaii International Conference on System Sciences, January 2011

[13] W. Liu, "Integration of Wireless Access and Wireline Networks: OAM&P Architecture with ITU-tML Technologies", IEC Broadband Wireless Report, International Engineering Consortium, December 2004.

[14] ANSI (American National Standard Institute, "OAM&P Information Model and Services for Interfaces between Operations Systems Across Jurisdictional Boundaries to Support Configuration Management Customer Account Record Exchange", technical editors W. Liu and J. Ng from T1M1 Standard Committee, revisions of 1998, published in 1999.

[15] S. Kent and K. Seo, "Security Architecture for the Internet Protocol", IETF Request for Comments: 4301, December 2005

[16] W. Liu and et. al, "TCP/IP Tutorial and Technical Overview", IBM RedBooks, http://www.redbooks.ibm.com/abstracts/gg243376.html, December 2006.

[17] NRC (National Research Council), "For the Record: Protecting Electronic Health Information", National Academy Press, Washington, DC, 1997.

[18] J. Walker, et al., "The Value of Healthcare Information Exchange", Health Affairs, http://content.healthaffairs.org, January 2005.