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

Smart and Connected e-Health Lab for Standards Validation and Conformance

Smart and Connected e-Health Lab for Standards Validation and Conformance

W. Liu
School of Science & Technology
Georgia Gwinnett College

E.K. Park
VP for Research and Dean of Graduate Studies
CSU - Chico

U. Krieger
Computer Science in Communication and Networks
University of Bamberg

S.S. Zhu
Department of Computer Science
Shantou University

***Abstract*—This paper reports our innovation in a Smart and Connected e-Health Service (SCeHS) lab approach for e-Health standards validation. The lab platform has been designed for SCeHS which is a next generation solution following the initial Big Data e-Health Service (BDeHS) initiative. After a number of e-Health standards are summarized, we present our validation designs for conformance to those e-Health standards.**

Keywords—Smart-and-Connected e-Health; e-Health Lab Platform; e-Health Services; Flow Validation; e-Health Standards Conformance

I. INTRODUCTION

The purpose of Smart and Connected e-Health Service (SCeHS) program is to develop next generation healthcare solutions to improve patient outcomes, decrease costs, and address the complexity of challenging e-Health problems in interconnection infrastructure, data processing flows and security all following a number of regulations and standards.

Our pursue of e-Health fundamental research is to enable interoperable and scalable infrastructure, applications, and services for effective sharing and usage of electronic health record data, data representation including semantic metadata, and networked applications that access such data. We investigate aspects of a continuously scalable universal exchange [1] for current and future e-Health with data originating from diverse sources in multiple formats and standards. We have developed advance network processing methods [2,3] for controlling and maintaining data integrity, provenance, security, privacy and reliability of original as well as aggregated data. Furthermore we research architectures [4,5,6] for trustworthy patient identification and authentication and access control protocols, in order to maintain sensitivity to the legal, cultural and ethical issues associated with securing e-Health data[7,8,9,10].

This paper reports our lab R&D approach for e-Health standards validation when dealing with new e-Health services and application flows. The e-Health LAB platform consists of the infrastructure layer, a tool set platform, a functional layer and the e-Health resource layer, connected via data virtualization and exchange protocols, for the purpose of application flows and e-Health service development and deployment with quality of service controls. One immediate application is an innovative design to validate e-Health standards implementation as well as to validate compliance.

II. SMART AND CONNECTED E-HEALTH LAB PLATFORM

A. *Smart and Connected e-Health*

Figure 1 below depicts an environment that creates, validates and deploys e-Health application flows by combing e-Health solution framework with an innovative test bed and deployment platform.

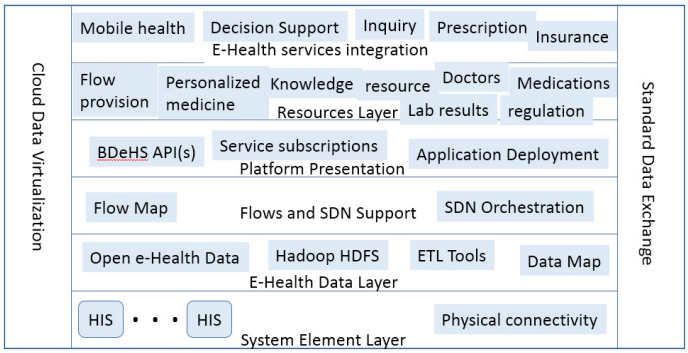

Figure 1. ***e-Health Lab Platform Architecture***

After the initial framework of e-Health interconnection solutions presented in [1~5,9,11] where networking and communication services are the primary objectives, our new lab approach will maximize the data transformation and exchange capabilities. Standard data exchange is augmented by an overarching data service strategy with the ultimate goal of converging the service provider centric record into a patient-centric and patient-owned records for treatment, medication, billing and holistic case histories that are beyond PHR (patient health record). The detail technology will be reported in a separate technical paper.

To achieve the goal of big data e-Health services and transformation, the data relationship are extended into the system element layer where each element will represent a complex HIS/CIS/RIS/e-Subscribe and CPT healthcare billing with regulatory requirements such as HIPPA/HITEC as well as archives of EMR, NCPDP, LOINC, SNOMED,

PACS, DICOM, and insurance records. Due to diverge sources and varying format structures, data maps and processing tools are included in the e-Health data enhancement layer.

Although we minimize the physical connectivity with external HIT systems in this lab environment, the networking service layer still play a key role in development of new services of this platform as various network deployment scenarios have to be considered when the applications and services are to be deployed into production HIT environment. As such, a number of flows and software defined networking controls are going to be incorporated along the way while we are perfecting the data-centric platform.

A number of e-Health resources beyond the data models and connectivity controllers are being developed to facilitate innovative e-Health service flows, mobile health interfaces, security control and audit functionality and additional Big Data resources. The smart and connected big data functions are formulated into Big Data e-Health Service (BDeHS) APIs for planning evidence-based programs, for predicting disease onset to intervene earlier, for delivering the right case services to support the individual with the exact treatment to improve quality and for optimizing e-Health care resources.

Integration engines of this lab platform are to achieve Level 5+ [12] and go beyond of "Machine-interpretable data transmission of structured messages containing standardized and coded data; idealized state in which all systems exchange information using the same formats and vocabularies". The integrations allow rapid roll out of application services into various e-Health application domains.

B. e-Health Standards

The U.S. Department of Health and Human Services published the Final Rule [6] for Health Information Technology that included standards of implementation and certification criteria for e-Health technology, which required security context management to accommodate more types of patient data being efficiently shared and further expansion of access to patient data due to accelerated conversion of data into useful intelligence. The Final Rule listed the functions or services and promoted enhanced interoperability, functionality, utility, and security of EHR technology. Our lab platform is in the process of enhancement through the capabilities they include and the standards to meet for certification to demonstrate Meaningful Usage of e-Health technology in improving health care.

HIPAA (Health Insurance Portability and Accountability Act) [13] included privacy and security rules that became effective in 2005. It required that privacy data must be encrypted and health practitioners must destroy unencrypted copies of health information after use. Medical data used for research must be limited to the information relevant to the study and with adequately obscure patient identity.

The legitimate entities or CE (Covered Entities) that may directly use e-Health information records include a Health Plan, a Healthcare Clearinghouse, or a Healthcare Provider that transmits electronic data in a manner covered under HIPAA. If one covered entity wishes to transmit protected health information to another covered entity for purposes of health treatment, payment, or operations, it is permitted to do so.

The HITECH (Health Information Technology for Economic and Clinical Health) [14] legislation was passed in 2009 with additional monetary incentives to interconnect the e-Healthcare systems with majority of hospitals and clinic offices by this decade. The HITECH legislation extended the previous HIPAA legislation and further outlined plans for required privacy and security controls on digital healthcare systems. HITECH includes the addition of new requirements on reporting breaches. Additionally, HITECH increases the severity of HIPAA penalties for both inadvertent and willful disclosure of unsecured patient information. The fines under HITECH increase with the severity of information security violation (up to millions of dollars).

HITECH also extended the requirements beyond parties covered under HIPAA to include Business Associates (BA). In cases where a covered entity wishes to transmit health information to a non-covered entity, such as a software vendor, a Business Associate Agreement (BAA) is required. A BAA should address security risks including (1) Insider curiosity: Associates abuse their record access privileges out of curiosity or for their own purposes; (2) Insider subornation: Associates knowingly access information and release it to outsiders; (3) Uncontrolled secondary usage: Those who have access rights to patient information for the purpose of supporting primary care may exploit that access for other purposes not envisioned in patient consent forms.

Electronic Medical Records (EMR) is defined as an application environment composed of the clinical data repository, clinical decision support, controlled medical vocabulary, order entry, computerized provider order entry, pharmacy, and clinical documentation applications [15]. This environment supports the patient's electronic medical record across inpatient and outpatient environments. It is used by healthcare practitioners to document, monitor, and manage health care delivery within a care delivery organization. EMR also provides a variety of functions for organizations not involved directly in care. Records are sent to insurers (government and private) to justify payment for medical services rendered and to detect fraud. They are used for quality reviews, administrative reviews, and utilization studies to manage the business aspects of health care. And they are used for societal purposes, such as medical research, public health management, social service and welfare system management, law enforcement, screening and licensing for professions, and determining life insurance eligibility.

From the pharmacy services sector of healthcare, NCPDP [16] standards are used in pharmacy processes, payer processes, electronic prescribing, rebates, and additional focus on health care and pharmacy business solutions. The most successful SCRIPT Standard provides the following functions:

- Exchange between prescribers, pharmacies, intermediaries, payers
- New prescription request
- Change of new prescription
- Cancel of prescription
- Refill/renewals request/response or Resupply in long term care
- Fill Status notification
- Medication history exchange
- Drug Administration exchange in long term care
- Prescriber-reported samples for more robust medication history
- Query functions for new prescriptions

DICOM (Digital Imaging and Communications in Medicine) is the standard for radiology image exchanges [17] that are implemented in cardiology imaging, radiotherapy devices (X-ray, CT, MRI, ultrasound, etc.), and increasingly in devices in other medical domains such as ophthalmology and dentistry. There are literally billions of DICOM images currently in use for clinical care. DICOM has enabled medical imaging applications to advance clinical medicine.

Besides the medical domain specific standards, out lab platform design supports the ISO/IEEE suite of protocols and messaging standards for digital health monitoring and diagnostics devices [18]. In addition, our platform is also going through the enhancement process in order to conform the emerging EU standards [19]. Other emerging Asia e-Health standards are still under development. For example, during the Beijing HealthCom-2012 keynote speech, representative from the China Health Service ministry presented a grand vision of 3-tier health information deployment plan. Once those standards become available, our lab platform has to be further validated to meet those flows and standards as well.

III. E-HEALTH FLOWS AND CONFORMANCE

Our lab platform supports the capabilities to include e-Health standards for certification to demonstrate Meaningful Usage of e-Health technology in improving health care. The LAB e-Health data process flows are designed to use Systematized Nomenclature of Medicine (SNOMED) Clinical Terms, the International Codes of Diseases (ICD) and Health Layer Seven (HL7) standard format for export and import of health history and conditions on a patient's problem list. The interexchange of data is designed to utilizing standard vocabularies in XML format.

Another consideration of the LAB processing flows involve the element level systems or connection interfaces to those health information systems such as Outpatient Information Systems (OIS), Inpatient Information System (IIS), Emergency Information System (EIS), and Laboratory Information System (LIS) as well as the Radiology Information System (RIS) with the PACS (Picture Archiving and Communication System). Other flows have to be supported at the elementary level include Computerized physician order entry (CPOE) is an application that is used to electronically link with Clinical Decision Support Systems (C-DSS) to cover the steps in the flows of Order Entry, Order Confirm/Receipt, Order Review/Perform/Record, Order Query and last but not least Billing.

Big Data processing also guides application flow set-up procedures that detail the processing stages including data fork points, stream joints, as well as event and message logging. All of which are specified in a policy format that controls the in-flight processing of data. A protocol command (e.g., transform/send/store data) may be triggered by a protocol type and the policy ID established during the flow setup processing. A data flow in this e-Health environment is mapped into a stream with additional processing stages. In addition, aggregated data reports can be generated at any stages of the e-Health data streams.

In between the data entries and exits, a number of middle storage and processing stages supply data replications and parallel processing logics for additional data segmentation, summarization, (security and health regulation) policy enforcement, filtering, data transformation, header and trailer expansion, message split or union, state synchronization, and coordination with other distributed processing nodes. The in-flight processing allows flexibility to deal with regionalization and/or globalization standard conformance. External data will come from different medical systems in various regions and countries. Effectively working across these disparate data repositories can help identify any gaps in different regional standard implementations.

All the processing flows have to be organized as practical applications if the lab approach can be adopted for wide application usages. And to comply with e-Health security, privacy and trust, security controls become an integral part of the overall platform design. The application domains and security solutions are briefly presented here for the purpose of completeness and the details are intended to be reported out in a separate paper publication.

A. Application Domains

Our lab design accommodates the different service context management for various providers (the so called covered entities and their associates) and patients. There are large numbers of communication flows that go beyond a dedicated end point for patients. In addition, we have to consider multiple domains across multiple industries (that go beyond the core healthcare providers and patients).

Key domains include Electronic Health Records including data interoperability, security and privacy. Another domain is big data medicine where personal genetic markers in DNA assist in disease prevention, diagnosis, and treatment decisions, has continued to progress. The third domain includes remote clinical care, diagnostics, and electronic patient monitoring driven by the pervasiveness devices and wireless capability, by the relative affordability of devices, and by new remote clinical care technologies that enable doctors to provide medical assessments and treatments from

a remote location away from the patients without onsite specialist medical doctors.

Additional application domains include personalized medicine, which is combined with e-Health computing and genomic technologies to utilize information about a person's genes, proteins, and environment to prevent, diagnose, and treat disease. Clinical decision supports, operational quality monitoring, insurance and billings are all interested components of our application domains.

For flexible scheduling and routing of re-configurable flows with various lab interconnections, a software defined and application-oriented network orchestration and control framework allows our lab to replicate a data center environment with simulated service providers involved all the e-Health flows. This rapid deployment technology will support policy-based interfaces between domains of covered entities and between application flows and the control components of a domain. SND allows scale and avoids state explosion as the deployment grows with more (external) data center domains. And it supports tiered domains using different networking technologies.

B. Security Controls

Security Service Management provides a mechanism to secure information flows among three or more parties of different service provider roles or e-Health business associate roles following different policies governed by HIPAA or HITECH and the Health IT Final Rules. Our design of the lab platform allows different members (e.g., a provider or a secondary user) may have different authorization level from a subset of the e-Health information collections.

The (security) policies are in place before any external flows into the test platform are granted. When multiple entities are participating in a coordinated e-Healthcare process, they have to be checked against databases designed to implement the e-Health security framework [8].

The Security Policy Database specifies what security services are to be offered to the IP traffic, with rules such as types of source/destination 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 security manager modules. The Security Association Database contains parameter information about each e-Healthcare Application Flows, such as e-Healthcare routing algorithms and keys, protocol mode, and flow-level lifetime. For outbound processing, the selective encryption scheme has to be applied. All audit points will trigger to log the processing activities. Our solution requires that a logging mechanism be maintained in the cloud(s) that have access to both Identity/Certificate registration information as well as its own log repositories.

Another key security function is to de-identify patient from all flows. The ultimate goal of supporting the Meaningful Usage of e-Health records require at least the following contents in the communication payload (Patient name, Sex, Date of birth, Race, Ethnicity, Preferred language, Smoking status, Problems/Symptoms, Medications, Medication allergies, Laboratory test(s), Laboratory result(s), Vital signs, Care plan field(s) including goals and instructions, Procedures, and Care team members). Additional supporting messages could be derived from those sub-fields. For example, the information to a third party could include an Inpatient Summary or even a Medical Image using direct links to images stored in the EHR system. The de-identification process protects patient privacy and ensure the lab platform does not cause concerns in this regard.

Finally encryptions and authentications are integral requirements of this lab platform. Before any entity could be connected to the e-Health flows, a service profile has to be established for on-going authentication purpose. Each connectivity and subsequent flow modification are tracked from beginning to end of session. In conformance to the final implementation rules, our platform architecture solution enables encryption standards of e-Health as parts of our e-health security and privacy framework. This is to ensure all areas are sufficiently covered including cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference and compatibility; tests and design assurance; plus mitigation of other attacks.

In summary, the security mechanisms are to be applied to the various application domains under experiments. Current and emerging regulations and standards can be checked in the lab platform as key operational support capabilities.

IV. SUMMARY

The presented lab solution provides a platform to enable e-Health standards research, implementation, and validation of third party e-Health applications for compliance. Through an innovative transformation from diverse centric records and flow models into a holistic patient ownership design, it enabled a futuristic toolsets for data functions, e-Health resources integration, new service innovation, and validation of conformance to regulatory changes.

The operational capabilities form the foundation for future implementation of emerging standards, rapid data conversion and utilization, as well as rapid lab testing of new e-Health application flows. In addition, e-Health security, privacy and trust concerns can be enabled and validated for conformance through this lab platform.

REFERENCES

[1] W. Liu, E.K. Park and Udo R. Krieger, "e-Health Interconnection Infrastructure Challenges and Solutions Overview", IEEE HealthCom-2012, Beijing, China, October 2012.

[2] W. Liu and E.K. Park, "e-Healthcare Cloud-Enabling Characteristics, Challenges and Adaptation Solutions," JCM Journal of Communications, vol. 8, no. 10, 2013.

[3] W. Liu and E.K. Park, "e-Healthcare Interconnection Networking Services", JCM Journal of Communications, vol. 8, no. 9, 2013.

[4] W. Liu and E.K. Park, “e-Health AON (Application Oriented Network)”, Proceedings of IEEE International Conference on Computer Communication Networks, WiMAN Workshop, Nausa, Bahamas, August 2013.

[5] W. Liu, E. Park and S. Zhu, “e-Health PST (Privacy, Security and Trust)”Proceedings of ICCCN/MobiPST-2014 (Privacy, Security and Trust), Shanghai, China, August 2014.

[6] US Department of HHS, “Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology”, 2014 Edition.

[7] Technology Association of Georgia, “Big Data in Healthcare”, http://tagtvonline.com/tag-events/2013-big-data-in-healthcare, Atlanta, GA, June 2013.

[8] W. Liu and E.K. Park, “e-Healthcare Security Solution Framework”, International Conference on Computer Communication Networks, MobiPST-2012 (Privacy, Security and Trust), Munich, Germany, July 2012.

[9] W. Liu and E.K. Park, “e-Healthcare Services Characteristics and QoS Guarantee”, in ContextQoS 2011, 1st International Workshop on Context-aware QoS Provisioning and Management for Emerging Networks, Applications and Services, Maui, Hawaii, August 2011.

[10] E.U., “European countries on their journey towards national eHealth infrastructures”, Europe Union, 2011.

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

[12] J. Walker, et al. “The Value Of Health Care Information Exchange And Interoperability”, Health Affairs, 2005.

[13] US Congress, “Health Insurance Portability and Accountability Act”, 1996.

[14] US Committees on Energy and Commerce, Ways and Means, and Science and Technology, “Title IV - Health Information Technology for Economic and Clinical Health Act”, January 16, 2009.

[15] D. Garets and M. Davis, “Electronic Medical Records vs. Electronic Health Records: Yes, There Is a Difference”, HIMSS Analytics White Paper January 26, 2006

[16] NCPDP, http://www.ncpdp.org/Standards/Standards-Info, National Council for Prescription Drug Program

[17] DICOM, http://medical.nema.org, Digital Imaging and Communications in Medicine

[18] ISO/IEEE11073, “Medical/Health Device Communication Standrds”.

[19] E.U., “European countries on their journey towards national eHealth infrastructures”, Europe Union, 2011.

[20] 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.

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

[22] U.S. Department of Health & Human Services, “National Health Information Network”, http://healthIT.hhs.gov.

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

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

[25] US Committees on Energy and Commerce,Ways and Means, and Science and Technology, “Title IV - Health Information Technology for Economic and Clinical Health Act”, January 16, 2009.

[26] 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.

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

[28] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, and H. Luo, "Security and Privacy for Mobile Healthcare Networks — from Quality-of-Protection Perspective", Wireless Communications, IEEE, vol.22, no.4, pp.104-112, Aug. 2015.

[29] K. Zhang, X. Liang, M. Barua, R. Lu, and X. Shen, "PHDA: A Priority Based Health Data Aggregation with Privacy Preservation for Cloud Assisted WBANs", Information Sciences, Elsevier, vol.284, pp.130-141, Nov. 2014.