An Edge Device Centric e-Health Interconnection Architecture

W. Liu
GGC School of Science and Technology

E.K. Park
NC Central University

S.S. Zhu
Shangtou University

U. Krieger
University of Bamberg

***Abstract*—This paper presents our edge device centric architecture as a new system solution for internet e-Health objects interconnection and service delivery. The new approach was designed to enable new embedded health objects, to meet the growth in edge devices, to provide secure operations, as well as to establish a new e-Health interactive norms. It is going to enable the Internet of Things in the e-Health industry with diverse edge devices and embedded managed objects being integrated at the core interconnection.**

Keywords- healthcare devices; e-Health objects; interconnection architecture; security; service delivery

I. INTRODUCTION

The purpose of our e-Health research program is to develop next generation healthcare digital device interconnection solutions to improve patient outcomes, decrease costs, and address the complexity of challenging e-Health problems in security, reliability, efficiency and flexibility. In the past [1,2] e-Health devices were mainly managed in a local system by an operational personal with direct control but with minimum sharing or remote automations.

The emerging field of internet-ready e-Health medical devices brings revolutionary paradigms into the network of uniquely available healthcare devices embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data. The interconnection of those edge health devices outside the traditional healthcare systems are becoming to inter-operate across the Internet infrastructure in delivery of e-Health service, which in turn suggests the mandatory upgrades of the overall e-Health architecture solutions.

Furthermore, the integrated view of device connectivity and security and service delivery cannot be easily addressed by the traditional e-Health architecture as classical solutions are more focused on the needs of clinical/hospital/lab usages. As society is moving towards peer networking and on-line practices, it is imperative to combine the best parts of both the healthcare online networking services and the edge device technology revolution to formulate advanced e-Health solutions.

To provide a patient centric service with new e-Health devices and sensors, there is an urgent need to adapt the e-Health technological services to meet demand not only in numbers but also in improvement of social interactive norms. Recent advancements in e-Health research [3~12] have enabled interoperable as well as scalable networking, applications, and services for effective sharing of electronic health records, flexible data representation, and more efficient services that access such health data.

Our new initiate is to incorporate the edge devices as internet nodes in an integrated managed device object model with end-to-end flows and impacts in e-Health. This paper presents this new edge device interconnection architecture approach. It is organized as follows. In section II, we describe the e-Health device fundamentals. In section III we explain our overall architecture evolutions from the various phases of e-Health interconnection models starting from the basic digital healthcare towards the interconnected managed objects for the intelligent edge devices in the context of e-Health service delivery. Additional security models supplement the context management capabilities, regulatory compliance, and collect e-Health meaningful usages. The final section IV concludes with a summary of our contributions.

II. EDGE DEVICE FUNDAMENTALS IN E-HEALTH

In the context of e-Health, a series of medical devices and health fitness devices are available such as glucose monitors, pulse oximeters, weighing scales, medication dispensers and activity monitors. For continuing and acute care devices, there are pulse oximeters, ventilators and infusion pumps. Computer aided surgery and augmented reality further supply a new generation of devices that are BRILLO based or Azure IoT based with vendor specific connectivity models [13,14].

Before describing our edge device centric architecture design, let us review some technical features of those devices in the context of e-Health flows.

A certified medical device should provide e-Health data optimized for vital signs information representation based on an object-oriented data model. When integrated into the e-Health system, general service applications are expected in either service polls or event driven applications. For data adaptation purpose, internetworking and gateway standards allow observation reporting interface from IEEE standard messaging and data representation to HL7 or DICOM format [15~18]. Different category of the health devices are further summarized in the following.

A. e-Health edge devices

The key devices involved in a typical e-Health can also involve processing some subset of the fields of Electronic

Medical Records, Electronic Health Records, e-Prescribe, a Lab request and report including simple blood test and complex DICOM images. Specifically for applications, they are classified in the following categories.

- Remote health monitoring: Special healthcare data from medical cards of patients in a real-time mode. They allow doctors to conduct analysis, send notifications to suppliers and patients;
- Wearables: These gadgets are continuously monitoring daily activity of patients, and they can inform about steps taken, burnt calories, heart rate etc. They help prevent some dangerous conditions when emergency is required;
- Patient-oriented medicine: This medicine includes devices that can provide medical care considering all individual particularities and demands of each patient using healthcare sensors;
- Maintain vital equipment: It allows specialists to provide the proper functioning of vital medical devices when your patients need them most. Thus, it helps fix all problems with the maintenance in advance.
- Medical assets monitoring: It helps medical employees spend less time on searching and other additional tasks, so they will be able to spend more time with patients due to the improvement of medical assets monitoring and managing them. So IoT and healthcare can be mutually beneficial for each other.

B. Medical Device Standards

The foundation standards to govern the medical devices and connectivity in particular are still the ISO/IEEE 11073 standards [19].

The standards have been included in the USA National Committee on Vital and Health Statistics recommendations to the Department of Health and Human Services related to patient medical record information message formats supporting Health Insurance Portability and Accountability Act (HIPAA) [20] compliant implementations.

Besides the basic communication information models for each domain, the same set of ISO/IEEE 11073 standards also supplies Part 20101: Application profile – Base standard, Part 30200: Transport profile – Cable connected (amended), Part 30300: Transport profile – Infrared wireless, Part 30400: Transport profile – Cabled Ethernet, and Part 90101: Analytical instruments – Point-of-care test.

C. Peer Transmissions

In the traditional medical device model, communication occurs directly between peers instead of through a central node. Each node stores and forwards information to all other nodes. In healthcare activities, device records no longer have to be shuffled around via a huge admin center or insurance. Instead each entity posts the activities involved to the e-Health system. Once they are validated and agreed upon via the appropriate protocol, the admin center and insurance companies become a pure consumer of the original e-Health activity data blocks. In the IoT paradigm, additional interconnectivity among millions of devices can enhance the healthcare service delivery model within a global scale.

D. Provision and Tracking

Every medical device has to be provisioned inside an e-Health solution so that it is constantly tracked. The most relevant step is the generation of a managed object regarded as the "DNA image" of the devices with initial setup states. Subsequent operation can be modeled on the objects. For reporting purposes the object behavior are traced and tracked.

E. Managed Device Objects

A managed object (MO) enables the corresponding device be activated, deactivated and constantly adjusted. Once a MO is entered in the database and the accounts are updated, the records cannot be altered, because they are linked to every transaction record that involves a particular device. The MO containment tree allow the devices to be named in a unique way, which allow all devices to be coordinated in a core interconnect solution. Various computational algorithms and approaches are deployed to ensure that recordings in the database are permanent, chronologically ordered, and available to all others on the network.

F. Edge Flows with End-to-End Logic

Service flows from edge devices to service providers are tied to computational logic and in essence programmed so users can set up algorithms and rules that automatically trigger transactions between managed devices. The embedded procedures cover security audits, regulation compliance reporting, billing updates, medication allergy alerts, over-prescription thresholds and personalized medicine tied-in to a specific patient cure flow as prescribed in an accepted cure procedure. Deviations are detected and flagged because of end-to-end logics prior to device deployments. Those end-to-end logics prevent the edge devices from becoming autonomous healthcare delivery islands. Instead side-effects, allergies, medication conflicts and over-doges become a part of the overall health service flow activities. All the service flows enable a central orchestration engine to optimize the care process while collecting global data to validate the cost effectiveness of care procedures that involve a large number of automation medical devices.

III. E-HEATH EDGE DEVICE INTERCONNECTION

As the core e-Health systems are relatively stable, rapid growth comes from medical devices in the edge as well as embedded IoT entities in the patient end points. While we retain the e-Health core components from present e-Health solution systems [3~12], the enhancement with medical devices mandates new protocols both within a realm and adaptation inter-domains. We also have added an Edge Device e-Health Integration Engine (EDeHIE) for enhanced end-to-end flows as well as safety and security operations. EDeHIE aims at maximizing core module standardization in the architecture series. For example, the architecture solution retains the initial security framework as well as the native regulatory reporting conformance. And the new edge interfaces allows flexibility of integrating next generation of

medical devices management at the operational the center. Patient IoT devices will follow the same managed object model in our future extensions.

At the very beginning of our e-Health solution design, the fundamental DHC (Digital Health Care) architecture [3] originated from the Service Layer solution over networked e-Health systems as illustrated in figure 1 below. Since then the design has also evolved from network interoperability solutions and e-Health security framework to cloud-computing and as well as fast development platforms [4~9].

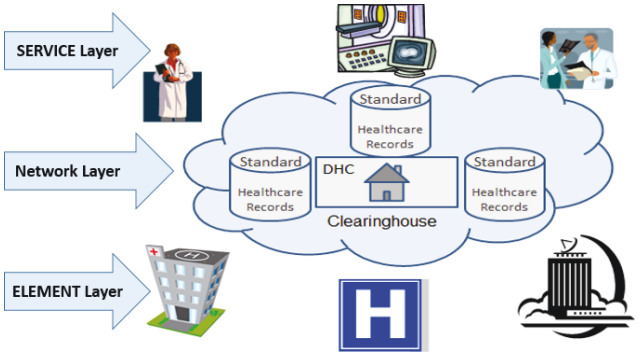

Figure 1. e-Health interconnections

As more and more devices were added into the development, the Smart-and-Connected e-Health Service [10] moved towards incorporating access devices and gateways into the mix. It was designed with context-aware networking capability allowing any application-oriented services to push security policies down to the network layer. Access devices and their adaptor gateways are regulated with the e-Health security scheme to facilitate dynamic fork/join of the e-Health network flows. Cross-layer management furthers enhances provisions with centralized security service management, which guarantees cross-layer performance as well as security assurance.

Another major architecture advancement is the BDeHS [11,12] approach for the big data e-Health model that provided trustworthy patient identification, authentication and access control protocols, maintaining the sensitivity to the legal, cultural and ethical issues associated with a variety of universally accessible e-Health data (structured, semi-structured and unstructured) from variable data sources.

While most of the system architecture could be preserved, a large number of peripheral devices in e-Health are shifting many of the processing points towards the edge of the infrastructure. As the number of healthcare data processing points grows exponentially on the outset, smart edge e-Health is tilting the architecture solution towards device connectivity, data sharing, and service flow orchestration. Our response to this demand is the integration of devise managed model to follow the strict security, safety and operational requirements in the healthcare industry. e-Health Device Orchestration Protocol

Medical devices are conformant to the ISO/IEEE and security standards during manufacturing process [19,20]. When integrating into the e-Health service flows, additional rules govern the further interactions with the e-Health system environment. For each device, a check list will decide on the communication payload contents as well as how to process the payload during task completion. For example, most of the devices may not have enough RAM to store the patient IDs of those using the devices. But if they do store the session information with patient IDs, HIPAA rules [20] shall take precedence in protecting privacy.

These protocols mandate the inclusive device ID(s), the corresponding signatures from the e-Health service providers and/or the patients acknowledging to the acceptance of care. The same protocols can involve any subset and combinations of the existing HL7 messages, Lab LOINC codes, ICD codes, e-Prescribe as well as. Figure 2 below is an illustration of the orchestration in adding the devices via managed object models.

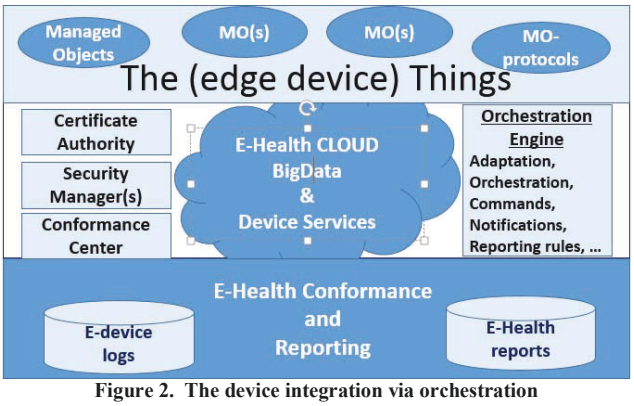

Figure 2. The device integration via orchestration

The orchestration protocol allow exchanges of device IDs and permissions, notifications by medical devices within an ownership realm, and commands in service delivery. Permissions can be expanded for government agencies and auditors, who may need access to more healthcare detail. Having an integrated management with a single source of truth improves the ability to monitor security and audit the cares.

Another key state in the orchestration protocol is during the provision process when a medical device is turned live with patient care flows. The managed object that characterized the device session are constantly updated with vital signs and activity logs for constant monitoring for conformance to the pre-agreed care flows in the core systems. Accidental failures and malwares are detected in real time with designed methods and procedures.

Some of the healthcare edge devices play a supporting roles rather than directly delivering care tasks. The protocols for provisioning those supporting entities still create managed objects to ensure correctly disease detection, medicine control in supply and intakes, maintenance of medical devices, and so on.

A. Inter-Domain Adatations

Before each device-generated stream (aka, the protocol message sequence) is incorporated into e-Health records to document activity, adaptations into a common block syntax is required for healthcare service providers and patients alike

to post those messages. Adaptation gateways serve this purpose such that requests and responses are reformatted accordingly with API calls through an e-Health cloud. Inter-domain service means multiple service providers can now deploy their certified devices in collaborative care for the same patients without moving the patient from facility to facility. The diverse e-Health data sources is illustrated in the figure 3 below.

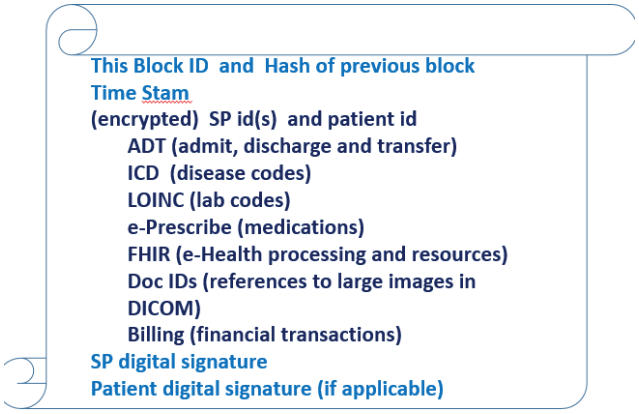

Figure 3. e-Health Data Sources

B. Edge Device e-Health Integration Engine (EDeHIE)

As medical devices and embedded software adaptors are becoming an integrated systems of e-Health flows, the overall EDeHIE orchestration engine provides healthcare specific logics to trigger smart transactions (aka actions in the medical devices) defined as a proven treatment procedure flows with maximize automation in mind. The engine provides essential support to other operational functions in the following categories.

- adaptation rules,
- orchestration of service logics,
- decision rules and processing supports, and
- regulatory compliance rules to drive other additional services such as reporting, discovery and research.

C. EDeHIE Security Operations

The Security Policy Database specifies what security services are to be offered to the IP traffic, with rules such as types of sources/destinations 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 flow, 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. 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.

Once a secure e-Healthcare association is established, both end points may invite others to participate in a shared care processing. Therefore, the related processing logs can no longer be kept in separate repositories (possibly even belonging to different clouds). 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.

D. Regulatory Conformance

The solution of EDeHIE design has to meet the stringent privacy specifications as required in HIPAA [20] and subsequent rules [21]. Through the use of IDs and permissions, patients can specify which part of e-Health record details they want others to be permitted to view when they are flowing through the EDeHIE care service sequences. Permissions can be expanded for government agencies and auditors, who may need access to more healthcare detail. Having a centralized but shared data collections can serves as a single source of truth with the ability to monitor security and audit the cares.

Additional value-added service systems are derived from accessing to the new EDeHIE generated data. For example, a supporting entity such as insurance may obtain identification information and extract and process the e-Health blocks as referenced by a billing message chain without the physicians to submit billing requests as in existing flows. These activities are in turn automatic because of the computational logic in e-Health flows automatically trigger billing processing and payment transactions between nodes in insurance and in a doctor's office. As another example, various reporting services can be supplied when working with the EDeHIE service engine after appropriate compliance rules are provisioned and constantly updated. Additional value added applications can be extended to health care research and discoveries.

IV. BENEFITS AND LIMITATIONS

The key benefits are multifaceted in extending the e-Health architecture approach to include the edge devices as the centric focus with anticipation of growing healthcare internet devices. We position the solution as a major step of e-Health architecture evolution to incorporate the fast growing medical devices and thus expand on the inclusive domains/reach of e-Health systems.

The expansion of medical devices and corresponding managed objects would allow integrated processing of auto health service delivery to reduce cost. In this solution, we place them directly into the domain of patient care where the external edge devices (as oppose to the e-Health systems) are playing a central roles in parallel to physician care and human intervention. Our solution provides end-to-end healthcare flows while preserving patient privacy and security.

The growing large number of developers as well as the high interest levels in the internet of things for medical devices will eventually push the edge device integration into a well-accepted mode of operation into the e-Health territory. Our solution is also a good attempt to further improve

efficiency and reliability as inherently derived from the inevitably growing trend of smart and reliable edge devices into the e-Health domains.

With extension for medical device orchestration protocols, computational logics have been embedded to the e-Health flows. Additional personalized medicine is enabled by the complete and consistent remote medication endpoints available for all service providers involved. The EDeHIE engine stands ready for the embedded security audits, regulation compliance reporting, billing updates, alerts from lab results and medication events. Innovative healthcare services with e-Health devices will eventually emerge from the new e-Health practices.

The edge device integration are further propelled by the readily available medical device solutions to automate, monitor and intervene as well as AI (Artificial Intelligence) technologies. The automation from using EDeHIE architecture solutions not only enhances efficiency but also enables innovation of new types of e-Health service flows into the future.

Yet a number of unknowns can still potentially limit the fact and wide spread of this solution approach. The first one is in the regulation concerning uniform rollouts and leveling the fields. Another potential concern is that the industry could emerge with competing integration platform implementations to cause interoperability gaps. Finally, the capturing of interactions between the edge e-Health devices and the service providers are not yet standardized. Future flows have to be migrated to the inter-service events using the Patients as focal points, which may not be the case when a vendor only focuses on its own device proprietary technology.

Even with these challenging limitations, we are still very confident with this direction to realize the edge device centric interconnection via the EDeHIE solution. Most significantly, our direction in expansion of the devices into the e-Health solution are aligned to the ultimate purpose of the callings for digital health priorities around the global world [22~24].

V. REFERENCES

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

[2] M. Braunstein and B. Todd, “Disruptive Technology in the Healthcare Space”, GaTech Seminar on technology innovation in the healthcare space, Atlanta, Georgia, on Febuary 10, 2016.

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

[4] W. Liu and E.K. Park, "Emerging Platform for Healthcare IT Services", Proceedings of International Conference on Computer Communication Networks Workshop, Zurich, Switzerland, August 2010.

[5] W. Liu and E.K. Park, "e-Healthcare Cloud Computing Application Solutions", Proceedings of International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium, San Diego, CA, January 2013.

[6] 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.

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

[8] W. Liu, “Advanced block-chain architecture for e-health systems”,IEEE HealthCom-2017, Daling, China, October 2017.

[9] W. Liu, T. Mundie, U. Krieger, E.K. Park and S.S. Zhu, "Rapid delivery e-Health service (RDeHS) platform”, Proceedings of HealthCom-2016, International Conference on e-Health Communications, Services and Applications, Munich, German, September 2016.

[10] W. Liu, U. Krieger, E.K. Park and S. Zhu, "Smart and Connected e-Health R&D Platform: A Lab Approach for e-Health Research and Development”, Proceedings of HealthCom-2015, International Conference on e-Health Communications, Services and Applications, Boston, MA, October 2015.

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

[12] W. Liu and E.K. Park, “Big Data as an e-Health Service”, Proceedings of IEEE ICNC2014, International Conference on Computing, Networking and Communications, Honolulu, Hawaii, February 2014.

[13] Google Android Things, also previously known as the Brillo Internet of Things. https://developer.android.com/things/index.html

[14] Azure IoT Suite, https://azure.microsoft.com/en-us/suites/iot-suite.

[15] Health Level Seven International, http://www.HL7.org/implement/standards.

[16] Health Level Seven International, http://www.HL7.org/fhir.

[17] Digital Imaging and Communications in Medicine (DICOM), https://www.dicomstandard.org.

[18] NCPDP, National Council for Prescription Drug Program, http://www.ncpdp.org.

[19] ISO/IEEE11073, “Medical/Health Device Communication Standards”, 2004(base standards) to 2018(additional parts and revisions).

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

[21] 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.

[22] J.P. Hu, “Informationization Strategy for Supporting Medical Reformations”, IEEE Healthcom 2012 Keynote Speech, October 11, 2012.

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

[24] US Department of HHS, www.hhs.gov 2009~2017.