# e-Healthcare Interconnection Networking Services

Wei Liu[1] and Eun K. Park[2]
[1] Georgia Gwinnett College, Lawrenceville, GA 30043, USA
[2] California State University, Chico, CA 95929, USA
Email: wliu@ggc.edu; ekpark@csuchico.edu

***Abstract***—The research effort for a national e-Health interconnection infrastructure and for the needs of supporting design guidelines is in great demand. Additional researches in e-Healthcare network services are critical to universal deployment in operational and security service management aspects. This paper presents our solution framework for e-Healthcare interconnection infrastructure, operational management services with security control, QoS guarantee, and new networking services creation. In the interconnection arena, we take into consideration to incorporate service management, on-demand access, quality-of-service accounting, and system interconnection requirements. In the security realm, our results include an e-Healthcare network security solution that enables multi-party participation, allows variable visibility into selective parts of data, and guarantees end-to-end security control. Altogether, our research provides a much needed innovative infrastructure framework to address the challenges and requirements as presented in this paper.

***Index Terms***— e-Health Interconnection, End-to-end Control, e-Health Service Security, Service Management, e-Health QoS Components, Service Creation and Operations

## I. Introduction

Digital healthcare solutions will transform the whole healthcare process to become more efficient, less expensive and higher quality [1]-[6]. The US government has pledged billions of dollars to help hospitals and clinicians develop and implement systems for digital health records and information sharing [7]. Independently, the industries also gear up developing information sharing technologies within the digital health networks. With additional significant investment by both private and public sectors, we expect that digital healthcare 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.

The key cornerstones of implementation include an interconnection infrastructure and Healthcare Information Technologies. A successful e-Healthcare implementation has to address a new paradigm in data transmission and information processing: from proprietary record ownership to networked consumption of health records; from distributed access of collaborative cares to centralized repository of portable records; from private information retrieval to security access control; and from ad-hoc IT solutions to orchestrated service creation and management. All aspects of the new paradigm shall impose new challenges in the underlying consumer healthcare communication and network infrastructure.

The core services are the foundation to exchange data among service providers and patients, as well as additional associations with business associates. The major exchange infrastructure enables transmission of electronic health/medical records covering patient demographics, progress notes, medication problems, prescriptions, vital signs, past medical history, immunizations, lab data and radiology reports.

In this paper, we point out the major challenges in various aspects of a national level e-Healthcare interconnection solution. By addressing those challenges, we formulate the solution requirements to have an end-to-end solution (reference architecture). To ensure practical deployment, we take into considerations to incorporate service management, on-demand access, quality-of-service (QoS) accounting, and system interconnection requirements. Our results also include an e-Healthcare network security solution that enables multi-party participation, allows variable visibility into selective parts of data, and guarantees end-to-end security control. 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.

From the network application standpoint, the interconnection infrastructure and networking services shall become enablers to revolutionize the roles and responsibility of the healthcare professionals as well as e-Healthcare consumers. Our paper further addresses next generation communication services that support pervasive healthcare applications together with additional operational management capabilities. We include solution capabilities for rapid communication session service creation by incorporating existing and new healthcare information network and operational capabilities.

The ultimate goal of our research is to supply an innovative solution framework reference that meets new e-Healthcare security requirements, achieving interoperable interconnections around various e-Healthcare parties. This paper reports our current research results and is organized as follows. Section II explains e-Healthcare background information that led into the e-Healthcare transformation movement. In Section III, we address challenges in e-Healthcare

Manuscript received July 26, 2013; revised September 20, 2013.
Corresponding author email: wliu@ggc.edu.
doi:10.12720/jcm.8.9.550-560

interconnection, security and QoS requirements. To meet those challenges, we describe in Section IV with multiple aspects of our solutions in interconnection service, security service, operational management, as well as the e-Healthcare connection service creation functions. Finally, Section V concludes with a summary of our contributions and future work.

## II. E-HEALTHCARE DRIVERS AND BACKGROUNDS

In early 2000's, healthcare IT systems were only isolate solutions that did not take the holistic view of healthcare process and outcomes. Major healthcare IT systems were explored in 2005 when the Certification Commission for Healthcare Information Technology (CCHIT) requiring vendors to update their records and systems to meet certification criteria.

A number of subsequent legislations with large incentives and technical advancements also provide the business drivers to further develop e-Healthcare solutions. The goal is to interconnect the e-Healthcare systems with majority of hospitals and clinic offices by this decade.

### A. HIPAA

HIPAA (Health Insurance Portability and Accountability Act) [8] 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.

### B. HITECH

The HITECH (Health Information Technology for Economic and Clinical Health) [9] 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.

### C. EMR

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 [10]. 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.

### D. PHR

Patient Health Record (PHR) provides a complete and accurate summary of an individual's medical history. Another name for PHR in digital format is called Electronic Health Record (EHR). According to [10], PHR is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports. The EHR has the ability to generate a complete record of a patient as well as to support evidence-based decision support, quality management, and outcomes reporting.

### E. NHIN

NHIN (Nationwide Health Information Network) initiative was launched with trials by about 4 vendors [11]. In the NHIN 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 a cyber infrastructure provides secure transport of existing clinical data from electronic health records. Additional e-Healthcare gateways may provide further connections with additional digital healthcare solutions. A simplified gateway with only local customized implementation is called an e-Healthcare adapter.

## III. E-HEALTHCARE IMPLEMENTAION CHALLENGES

In past several years, a number of initiatives have been reported to reform the healthcare IT systems, with a mix of success and failure results [3], [12], [13]. For example, in [3] a large-scale enterprise healthcare information system network infrastructure was implemented successful in the NTUH hospital. The transformation transfer from legacy systems was based on service-oriented architecture with a logical layer of exchange flow via Health Level 7 (HL7) middleware, Digital Imaging and Communications in Medicine (DICOM) standard, and the Healthcare Enterprise workflow. Preliminary performance showed reliability and robustness in that hospital traffic environment. To some extent it shared medical information easily among other branch hospitals, but lacked a national level interconnection solution which is the topic of our research in this paper.

In the IBM "Digital Healthcare 2015" initiative, the solution is beyond an enterprise healthcare system to include data governance, security and privacy solutions, information strategy, records retention, health information exchanges, hosted EHRs and enabling EHR plus for providers, etc. IBM predicted [12] that DHC (Digital Health Care) problems cannot be completely resolved without a new IT infrastructure impacting organizations, business, people, technology and processes. Another example is the Accenture NHS (National Health Service) project where the solution for NHS involved over 800 systems [13] but resulted in failure of the program. While the details of changes are not available and we could not find any architecture directions comparable to the other vendor's initiatives, the scale of that IT program supplied a numeric reference for future solutions.

### A. Interconnection Challenges

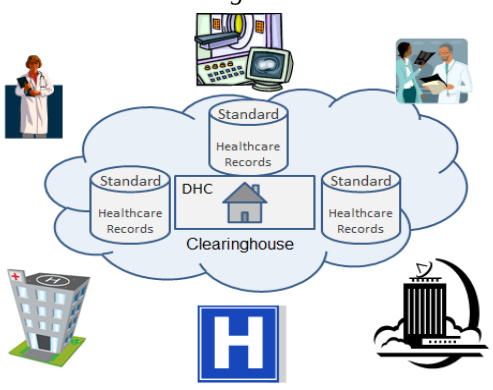


Figure 1. Basic interconnection environment

Fig. 1 below depicts an environment that supports access from individual outlets and test facilities as well as insurance providers and government agencies. All rely on a distributed repository of standard healthcare information records.

The major challenge is to ensure ubiquitous interconnection with the national health information networks. The following additional issues have to be resolved in order to accomplish associations, secure transfer flows, and effective 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 to ensure interoperability.

The interconnection protocol has to enable record generating functions as well as to coordinate activity interfaces. Multiple sources (and repositories) of data may be exchanged following an orchestration engine or following coordinated controls. In addition, interface standards and implementation guidelines have to be established. The complexity of a generic exchange (carrying) protocol has not been fully analyzed for existing NHIN trials [11] when abstracted from the specific healthcare data payloads. The issues of traffic loads and transmission patterns, which can impact system-performance and user-experience, have to be addressed.

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.

Secure exchange of service payloads and information flows have to be part of a solution. Possible messages include summary of patient record exchange, terminology mediation, message handling (includes transformation, routing, guaranteed delivery and content based filtering), secure data delivery, and confirmation of delivery.

### B. e-Healthcare Security Challenges

Security in the e-Healthcare is so critical that major deployments require security be a part of the solution along with functionality, interoperability and utility. The

universal reach and access of electronic medical records and personal healthcare information impose major challenges in the security architecture of e-Healthcare solutions.

As more and more healthcare providers are expected to convert internal data and transmit digital records over external infrastructure, passing through 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 [14]. And mandatory reporting on security violation will be imposed and audited.

When digital records can be easily shared, multiple parties are involved in e-Healthcare 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 studies [15] 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 e-Healthcare access infrastructure when electronic records are online. For example [16], even the Social Security Agency is participating in a trial to access electronic health record information for the purpose of determining evidence of disability claims.

At any time, many collaborating providers may possess variable visibility/right of the data. Some parts of the records are confidential patient personal information while other fields are epidemic information for public analysis and research. And still there are other portions 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.

Firms across all business sectors struggle with data security problems and it is unlikely that there is a prescribable solution that will work for all parties handling e-Healthcare 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 security solutions are summarized in the table below:

TABLE I SUMMARY OF SECURITY SOLUTIONS

| e-Healthcare Security Requirements | Existing (Point) Solutions |
|---|---|
| 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 Electronic Health Information for 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 to e-Health exchange network and applications. | 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. |

### C. QoS and Operational Challenges

To guarantee Quality of Service in e-Healthcare applications, we found it very challenging to combine (1) the healthcare applications, (2) the interconnection infrastructure support, as well as (3) operational support with common services. Only when a holistic understanding of all areas is established, we can better align our research in e-Healthcare interconnection services and end-to-end solutions with QoS guarantee. This is similar to the approaches in [17], [18].

The key QoS requirements for the e-Health infrastructure are listed below:

*1) QoS governing e-Health data communications*

A number of data communication channels may impose quality service parameters in the e-Health infrastructure. 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*

As in any communication session setup process, a number of resources and their availability can impact the response time of service collaboration.

Communication delays should be within a tolerable sub-second session setup time. And 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. When telemedicine becomes more pervasive, biosensors supplied the much needed data that have to be in synchronized with the consultation or treatment communications.

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 [19], [20]. 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, and continuous performance improvements).

## IV. E-Health Interconnection Solutions Framework

A new e-Healthcare infrastructure allows e-Healthcare records to be accessible by many parties involved in the process. Our framework solution enables multiple-party participations, allows variable visibility into corresponding subset of e-Healthcare records, and guarantees end-to-end controls. This solution also provides security control during association and transmission. In addition, a converged interconnection service creation platform is also architected to work with this infrastructure.

### A. Interconnection Infrastructure

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

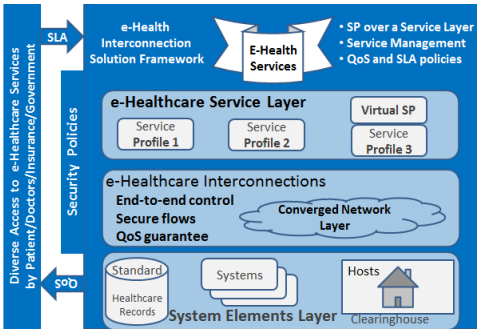


Figure 2. Universal e-Healthcare interconnection solution framework

*1) System elements*

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. A research-support system will gather, store and analyze patient medical information for use by researchers and for government (CDC) reporting. The research systems also

support new scientific discoveries, seeking better disease management regimes, monitoring public health. A patient-support system will gather, store and deliver medical information (e.g., PHR, EHR) to patient and doctors remotely, including medical history, allergies, vaccinations, appointments and invoices as well as inquiry supports.

*2) Converged network layer*

A converged network will link the underlying IT element system layer and a top service layer, while allowing pervasive access and ambient applications. The network architecture must support a policy-based system for managing network QoS and access device support for session enabled end points. 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. In order to support diverse access (anyone, anywhere, anytime), the converged network could be derived from a NGN (next generation network) infrastructure with integrated service support for healthcare data, medical images, telemedicine video sessions and other conference capabilities.

*3) e-Healthcare service layer*

Finally, the service layer is to present e-Healthcare industry standardized service interfaces towards to all partiers served by the digital healthcare infrastructure. 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 (SLA) 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.

To ensure a global end-to-end interconnection perspective and to uncover unintended threats that may not be available at the individual element level, our design solution for a security framework is described below. The design meets diverse processing requirements while being flexible enough to accommodate growing participants of the e-Healthcare revolution.

### *B. E-Healthcare Security Framework*

The current IPsec [21] protocol already provides integrity checking, authentication, encryption, and replay protection at the network layer. IPsec was designed for interoperability. It is independent of the current cryptographic algorithms, and it can accommodate new ones as they become available.

Our approach is to augment the IPsec capabilities with an adaptation mechanism (above the IPsec layer) to further enhance security adaptation in the e-Healthcare information routing. And we call this new approach as "Security association with service flow management".

In this 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 (Service Providers, Business Associates, Patients, Portal gateways, etc.), whether it is inbound, outbound, and so on. It contains an ordered list of policy entries one for each inbound and outbound traffic. 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. Those flows identify types of e-Healthcare service sessions (provider-provider, provider-insurance, patient-pharmacy, and so on). The purpose is to ensure multiple party participations in a controllable way.

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 e-Health Ports, or e-Health routing decision points of an e-Healthcare 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 e-Healthcare over NHIN will be backward compatible with our new e-Healthcare security framework. The adaptive security association enables secure interconnections for the following flows as defined in [15].

- Government Regulated Data Sharing: Certain government entities require the mandatory reporting of specific diseases. This reporting requirement clearly identifies the patient by name and demographic information as well as the medical conditions being reported.
- Insurance Data Sharing: Since insurance companies are often used to pay for medical treatment, the hospital is required to share any diagnostic and treatment information with the insurer.
- Connect to Dictation Services: As physicians treat patients, they often will dictate notes about the patient that 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. And the claims are sold to the collection agency at a fraction of the value owed.
- Supporting Services: A Hospital ABC has a relationship with a cloud-based server service for the purpose of scalable server services on-demand.

- Patient Portal Relationship: A patient portal allows a patient to log in to a web interface and communicate with their physician, view laboratory results, check invoices, and pay bills online. Data are sent to the patient portal provider through a secure channel, such as an encrypted feed.

Other connection relationships can be extended and enhanced on demand.

After a secure e-Healthcare association is established, both end points may invite others to participate in a MPMD (Multiple Participations and Multiple Drop-offs) e-Healthcare communication flow. The MPMD scheme was developed to address the issue of allowing different parties - to view a different subset of the records on-the-fly in order to collaborate in the care process, as illustrated in Fig. 3 below. The e-Healthcare Service Associates Identifiers are correlated together so that each entity has the visibility to the relevant portion(s) of the communication payload.

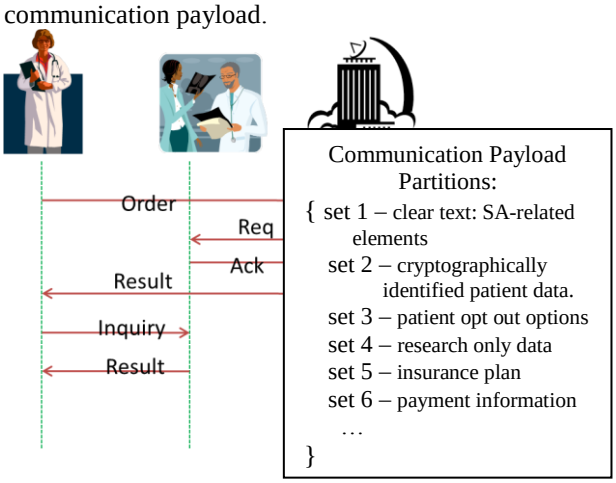


Figure 3. MPMD: Multi-Participants and multiple Drop-off points

While the issue of sending only a portion of relevant data set can be easily achieved in a port-to-point transaction environment, selective viewing is difficult to achieve in a multiple security association environment. With multiple parties in secure e-Healthcare association(s) and with their different roles and different access privileges to concurrently participate in the end-to-end e-Healthcare information networking, the potential growth of combinations is not scalable. This concern motivates us to come up with the following new solutions.

Here we partition EMR and PHR with multiple add-drop points along the transmission paths in the national health information network. We then associate the e-Health flow association IDs with access privileges to one or more data components to assure that only certain attributes (rather than a complete dataset of personal information) are granted to the right entity.

The e-Healthcare Service Associates Identifier(s) are correlated together so that each entity has the visibility to the relevant portion(s) of the communication payload. For example, Patient ID credentials (instead of the detail ID#, Name, Address information) are presented from Clinical offices to the Lab facilities. Sending only the essential (minimum) data that are pre-agreed upon among the e-Healthcare 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 e-Healthcare credentials.

The solution allows both individuals and the parties with which they're doing business to have higher-assurance transactions without needing to exchange the details of information that we usually do when registering with a new business online. This solution also 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 e-Healthcare market.

### C. QoS with End-to-End Control

The QoS service management solution was developed based on an integrated operational view of the interconnected e-Healthcare solutions. The total view is coordinated via an Operational Service Manager in collaboration with a Security Service Manager. The architecture (as illustrated in the Fig. 4) is explained below.

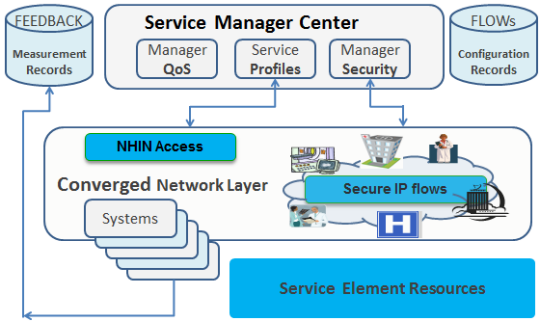


Figure 4. e-Healthcare operational support infrastructure

#### 1) Service centers

In our framework, a management center functions are applied to the QoS manager in order to manage the e-Healthcare service and network components as discussed below.

Service profiles define the operational policies and practices for subscription and provisioning of each communication component at the network layer. For examples, it should report delivered vs. contractual QoS. They include operational parameters such as network and resource performance and availability, but also encompass performance across all of a service's contractual or regulatory parameters. Failure to meet a contracted (Service Level Agreements) may lead to a Service Assurance Warranty payment. While the SLA is a user application policy, it can drive the interconnection level policies in the implementation.

To facilitate subscriptions, a directory service can be subscribed to the Service Centers. Specifically, e-Healthcare business scenarios and flows will drive the configuration of the (e-Healthcare) service flows.

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. Mediations or Message translation can occur at the network layer (for interconnection of diverse domains) and the translation of e-Healthcare messages can also happen at the service layer (for disease codes and procedure terminologies). The e-Healthcare manager has to be configured with the translations. Exception handling cannot exceed the predefined delay as defined in a service profile. The Operation Center continually monitors the overall performance indicators.

If necessary the service center can direct a QoS manager to divide the end-to-end service performance constraints (per session) into distributions among segments of networks. It may invoke switchover to redundant (data/voice/image-handling) resource components in order to meet e-Healthcare application and service constraints.

*2) Service resources*

The service management also provides "signaling" communication channels for interconnection infrastructure elements. The element resources are collection of nodes proving the monitoring and control functions. They support management of the network nodes and links. Each network component has to provide a view of each node and allows integration of network performance status and statistics.

*3) QoS service manager*

Control and coordination of the end-to-end network views will be the responsibility of the e-Healthcare QoS manager. For example, the e-Healthcare manager may enable partitioning and security to support the integration of network management information for instant provisioning on-demand. The QoS manager handles end-point performance parameter requests via an e-Healthcare application port. During a message flow, the QoS manager also monitors and assists in enforcement of end-to-end transmission performance, via accessing to logs and reports of functional performance feedback.

The QoS manager supports overall Service Managements similar to [19,20] to ensure that a specific e-Healthcare is performing according to specified performance 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-Healthcare service communication quality. The QoS manager may start re-initialization of session once additional communication and processing resources are recovered.

The QoS manager also addresses the tradeoff in capacity vs. loads, which led to admission control models. To fulfill this, futuristic models have yet to be developed for traffic mapping from upper e-Healthcare protocols to network transport traffic. Aggregation of correlated payloads into an encapsulated payload with same routing paths can be optimized between e-Healthcare partners.

*4) Service profile management*

Service profiles describe how to provision services for a specific domain or functionality such as e-Healthcare participation levels, messaging priorities, acceptable user parameters, end-to-end test setup, and so on. The services describe the specific interfaces to be used among interconnection participants to locate and exchange health information. All are governed by QoS parameters which in turn support patient service level guarantees.

At the operational level, additional e-Healthcare management profiles 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 PHR or other mechanism used to enter such preferences.
- 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.

*5) Security service manager*

When multiple entities are participating in a coordinated e-Healthcare process, the security associations will be managed by a Security Service Manager to coordinate the communicating groups. To further implement the e-Healthcare accountability requirements, we enhanced the solution framework with an end-to-end security control capability (called for any communication and information processing activities). An implementation of a security manager shall maintain three databases:

*a) Security policy collections*

The Security Policy Database specifies what security services are to be offered to the IP traffic, with rules such as types of source/destination (SP, BA, Patient, Portal, etc.), whether it is inbound, outbound, and so on. It contains an ordered list of policy entries one for each inbound and outbound traffic. 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.

*b) Security association flows*

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. 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.

*c) Distributed logs*

Once a secure e-Healthcare association is established, both end points may invite others to participate in a MPMD care processing. Therefore, the related processing logs can no-longer be kept in separate repositories belonging to a healthcare service provider. Our solution framework specified that a networked logging database be maintained by a set of collaborating agents that have access to both Identity/Certificate registration information as well as individual log repositories.

Furthermore, the management of the security service manager collaborating with service centers (described in the previous subsection) can provide the backbone implementation for any possible federal and state audits if any unwarranted e-Healthcare disclosures are discovered.

### *D. e-Health Connectivity Service Creation*

The most visible applications for practitioners are in electronic medical records exchanges. Furthermore, there are various clinical portals, ordering and medication management process automation, image storage processing, and numerous backend support applications including service coding tools, practice billing and financial processing. As for consumer-oriented applications in smart hand-held devices and terminals, we can expect the rise of pervasive healthcare applications such as access to patient health records during live consulting sessions, remote order entry, test status retrieval, pharmacy system, billing and payment processing. Additional healthcare research personnel will also be facilitated by the pervasive information retrieval and communication applications.

To best utilizing the underlying interconnection networking service infrastructure, a convergence service creation platform may become handy for additional value-added service providers. The platform would allow end-users (service providers and consumers) to produce session-oriented applications in supporting the applications listed in previous sections. As such, the systems are enablers to allow ubiquitous connections and creation of future pervasive healthcare application services.

The service creation platform includes the following major functions.

- A local NHIN access capability, augmented by secure flows within national health information exchange networks, accommodates end-to-end functionality between two cooperating entities (Service Providers to Service Providers) on behalf of a doctor, a patient, a lab or image diagnosis center, and/or administration staff.
- A service provision capability to rapidly setting up associations and direct the flows via the QoS management center. This functional module is to satisfy the requirements for interconnection interface conformance such as configuration, security setup, audit tracking and logging etc.
- Policy and security functions and usage accounting/charging functions. These are part of the overall operational management functional requirements. SLA becomes the driving parameters before any QoS manager makes a provision.
- A deployment portal to coordinate downloads of user services for patients (the e-Healthcare functions) and providers (the interconnection functions). The new updates may be pushed down to registered and participated devices as well.
- Data partitioning utilities to employ the intelligent logic of e-Health records. Data validator can be added to conform the e-Health standards, especially in the interconnection standards which are essential for interoperability of diverse access into the national level connectivity infrastructure.
- Audit reports to gather, store and analyze patient medical information for use by researchers and for government (CDC or Center of Disease Control) reporting. Security reporting capability to enforce and meet e-Health regulatory requirements.
- Other e-Healthcare IT functions may be exposed via existing IT application servers for non-standard provider specific applications in the billing, customer supports and business operation fields.

### *E. Limitation, Feasibility and Implementation*

There is practically no limitation in applying the architecture guidelines and reference models of this paper into variable e-Healthcare interconnections with end-to-end controls. The core set of technologies are feasible based on our experience in developing national scale interconnection services to exchange Primary Interexchange Carriers customer records [20] and as well as in implementing record portability in other similar industry. And the scale in those productions is comparable to the new e-Healthcare interconnections.

Those proven technologies are now adapted into a different context (e-Healthcare) with more rigid security and with similar operational requirements. Furthermore, the operational architecture can deal with requirements in supporting diverse service providers. That was the rationale driving the architectural directions.

As the e-Healthcare markets are emerging with new implementations, the service managers and overall solutions can be further extended to interact with other interoperable interfaces. To ensure wide adoption of this approach, a large scale development is under plan and they are due to be reported in subsequent papers.

## V. Conclusions

Our research has identified a need of a unifying e-Healthcare interconnection framework to ensure interoperability among different solutions. We have also identified and documented the security challenges and QoS requirements raised from ubiquitous access of the new digital healthcare functions. In this paper, we have presented an innovative e-Healthcare interconnection infrastructure to meet the challenges of new healthcare initiatives with interoperable interconnections, security controls and service level guarantees.

Our research resulted in a new direction with new distinguished features as follows:

- For the first time, an integrated view (of e-Healthcare application, networking service infrastructure and operational support) is developed and applied to healthcare pervasive IT applications, in contrast to all existing solutions that were 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 "e-Health transactions," and end-to-end security control).
- Our association management solutions are modular, letting service providers to build sophisticated application flows via identity systems using smaller and simpler subsystems in contrast to traditional ways of identifying all access end points. 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.
- Multiple collaborating parties in the e-Healthcare environment may be managed locally by a security manager working with variety of identity registration agents. The solution framework ultimately promotes a competitive e-Healthcare market place.
- A list of e-Healthcare QoS requirements is presented in this paper which includes communication services, processing flows and integrated management. A futuristic workflows and e-Healthcare messaging fields were also presented together with the layers of underlying processing infrastructure.
- A communication session creation platform allows rapid build-up of new e-Healthcare interconnection infrastructure, where convergence services across new communication platforms may become handy for additional value added service providers.

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 e-Healthcare interconnection infrastructure. The architecture provides a reference to achieve interoperable interconnections among various e-Healthcare parties or associated entities. And it could be dynamically reconfigured to satisfy large service providers to meet service guarantees.

Future works are planned to standardize the approach and map it into other emerging standards.

## References


[1] W. Liu, E. K. Park, and Udo Krieger, "e-Health interconnection infrastructure challenges and solutions overview," *IEEE Healthcom-2012, the 14th IEEE International Conference on e-Health Networking, Application & Services*, Beijing, China, October 2012.

[2] W. Liu and E. K. Park, "e-Healthcare security solution framework," in *Proc. IEEE International Conference on Computer Communication Networks*, Munich, Germany, August 2012.

[3] S. H. Hsieh, S. L. Hsieh, P. H. Cheng, and F. Lai. "E-Health and healthcare enterprise information system leveraging service-oriented architecture," *Telemedicine and e-Health*, vol. 18, no. 3 April 2012.

[4] W. Liu and E. K. Park, "e-Health service characteristics and QoS guarantee," in *Proc. IEEE International Conference on Computer Communication Networks, Workshop on Context-aware QoS Provisioning and Management for Emerging Networks, Applications and Services*, Maui, HI, August 2011.

[5] W. Liu and E. K. Park, "Emerging platform for healthcare IT services," in *Proc. IEEE International Conference on Computer Communication Networks, WiMAN Workshop*, Zurich, Switzerland, August 2010.

[6] W. Liu, "Digital health care (DHC) information technology infrastructure framework," in *Proc. IEEE Consumer Communications Network Conference*, Las Vegas, January 2010.

[7] IT World. (August 2009). [Online]. Available: http://www.itworld.com/networking/75306/us-pledges-12-billion-digital-health-networks.

[8] US Congress, *Health Insurance Portability and Accountability Act*, 1996.

[9] 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.

[10] D. Garets and M. Davis, "Electronic medical records vs. electronic health records: Yes, There is a difference," HIMSS Analytics White Paper, January 26, 2006

[11] U.S. Department of Health & Human Services: National Health Information Network. [Online]. Available: http://healthIT.hhs.gov.

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

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

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

[15] 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.

[16] Feldman, *et al.*, "Cyber infrastructure for secondary use of EHR Data: SSA's use of the nationwide health information network," in *Proc. 44th Hawaii International Conference on System Sciences*, January 2011.

[17] E. K. Park and W. Liu, "Wireless video services solution and management framework," *CCNC*, Las Vegas, January 2006.

[18] G. J. Wang, C. Z. Wang, A. Chen, H. Q. Wang, *et al.*, "Service level management using QoS monitoring, diagnostics, and adaptation for networked enterprise systems," in *Proc. Ninth IEEE EDOC Enterprise Computing Conference, International* , Sept 2005.
[19] 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.
[20] 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.
[21] S. Kent and K. Seo, "Security architecture for the internet protocol," *IETF Request for Comments: 4301*, December 2005
[22] J. Walker, *et al.*, "The value of healthcare information exchange," *Health Affairs*, January 2005.
[23] National Research Council, *For the Record: Protecting Electronic Health Information*, National Academy Press, Washington, DC, 1997.

**Dr. Wei Liu** received his Ph.D. from Georgia Institute of Technology in Atlanta, Georgia USA. He is a founding IT faculty member at the GGC School of Science & Technology in Lawrenceville GA. He researched and taught TCP/IP networks in the University of Maryland prior to his 10 (plus) years of technology leadership career in the industry, where he participated in a number of network transformation projects and service development integration programs. He also provided thought leadership for infrastructure development initiatives at major Technology Labs. He received awards for his contributions to industry and ANSI standards development. He coauthored with IBM the well-known book of "TCP/IP Tutorials and Technical Overview" with 1,000 pages of descriptions of Internet-related protocols and advanced applications back in 2006. Currently, he is investigating new infrastructure opportunities (in e-Health, government, military, network and service convergence, security, and other big data applications) that can lead to future offerings and new IT capabilities.

**Dr. Eun K. Park** received the PhD degree in Computer Science from the Northwestern University, Evanston, Illinois USA. He is the Vice-Provost for Research and the Dean of the Graduate Studies at CSU-Chico, where he is also a Professor of Computer Science. His research interests include computer communications and networks, optical networks, distributed systems, data mining, e-Healthcare infrastructure/architecture/ cloud solution, bioinformatics, information and knowledge management, and object-oriented methodology. He was the Dean of Research and Graduate Studies at CUNY-CSI. He served as a Program Director, CCF/CNS Divisions, CISE Directorate at US National Science Foundation. He is the founder of two conferences: ACM CIKM (Conf. on Information and Knowledge Management) and IEEE IC3N (International Conf. on Computer Communications and Networks).