Adaptive Governance on Electronic Health Record in a Digital IT era

Full Paper

Yoshimasa Masuda
Carnegie Mellon University, PA, USA
ymasuda@australia.cmu.edu

Donald S. Shepard
Brandeis University, Boston, MA, USA
shepard@brandeis.edu

Shuichiro Yamamoto
Nagoya University, Japan
yamamotosui@icts.nagoya-u.ac.jp

Abstract

An electronic health record (EHR) is a repository of information regarding health status and longitudinal electronic records of patient information. During the past decade, EHR use has grown in Australia significantly, while adoption rates of EHR across the United States reached more than 90%. To support this expansion, enterprise architecture (EA) is effective because it can contribute to the design of information systems facing major technical challenges in the era of cloud, mobile IT, big data and digital IT. Recent research proposed and verified the “Adaptive Integrated Digital Architecture Framework (AIDAF),” which can meet with IT strategy promoting digital IT. This paper highlights the existing inadequacies in the governance and management of current EHRs and investigates how the AIDAF can improve EHRs. This will be demonstrated by using a case study, interviews with government and hospital officials in Asia Pacific countries such as Australia, the United States region as examples. The AIDAF should contribute to enhancements of governance and management for EHRs toward the era of digital IT.

Keywords

Electronic Health Record, Digital IT, Enterprise Architecture, Digital Healthcare, IT Governance, EHR Implementation

Introduction

Many types of electronic health records (EHRs) exist worldwide. They are varied and operated by both the public and private sectors. EHRs can cover a range of data, such as medical histories, and laboratory test results, medications, allergies, immunization status, demographics, etc. For example, Australia currently operates a centralized electronic health recordkeeping system known as ‘My Health Record’ (MHR) — previously named the ‘Personally Controlled Electronic Health Record’ (PCEHR). The PCEHR/MHR system was designed by the National Electronic Health Transition Authority (NEHTA) with the Australian Government (Commonwealth of Australia, 2017). While the goals of this system are laudable, we found that their implementation do not meet current needs, with misalignment between the management of the information system and the knowledge management technologies (Payne et al. 2013). Health data collection and utilization are scattered and often disorganized in Australia as well (Commonwealth of Australia, 2017). Over the past decade, the context for EHRs has changed substantially. Major changes include new technologies, globalization, shifts in customer needs, new business models, and cutting-edge information technology (IT), building on cloud computing, mobile IT and big data technology (Boardman et al. 2015).

The term enterprise architecture (EA) encompasses all enterprise characteristics, such as business, organization, applications, data, and infrastructure. To meet current and future needs, we recommend that EA frameworks incorporate sufficient flexibility to consider emerging new paradigms, such as enterprise mobile IT, cloud computing (Buckl et al. 2010, Alwadain et al. 2014). Despite its desirable intentions, The Open Group Architecture Framework (TOGAF) has been criticized for its size, lack of
agility, and complexity (Gill et al. 2014). We argue that existing EA frameworks are not appropriate for digital transformation (Masuda et al. 2016). In Australia, for example, doctors’ clinics don’t agree on a common computer codification and software interoperability (Sue 2018). Public revelations exposed data security and patient privacy lapses, leading to the resignation of Australia’s EHR privacy chief to take responsibility for the issues (Ben Grubb 2018). To avoid such problems in the future, IT should be governed so that EA should have an important role in governing and managing EHRs in each IT project in related organizations to ensure alignment with an overall IT strategy.

The main purpose of this paper is to propose a framework to manage the EHRs in EA. Another purpose is to investigate effective elements to improve EHRs toward the era of digital IT. As an illustration, we use a case study of the up-to-date EA, incorporating interviews with government and hospital officials in Asia Pacific countries, such as Australia, Japan, and the United States region.

This paper is organized as follows: the next section provides the research background, followed by the description of research methodology and a summary of the case of applying AIDAF to improve EHR. Then, a framework for governance and management of EHRs toward the era of Digital IT is proposed. Next, the case of EHR in digital government and digital governance readiness for EHR across countries are discussed. Finally, conclusions and the limitations of current research and future research are outlined.

**Direction of EHR, Enterprise Architecture, Digital Healthcare**

**Background on EHRs**

Over the 50 years that followed the first implementation of computerized patient medical records in 1960s, technology advances in computer innovations opened the way for advancements in EHRs and health care (Turk 2015). The ISO standard defined an electronic health, healthcare record (EHR) as a repository of information regarding the health status of each care in computer processable form (International Organization for Standardization (ISO), 2005). EHR can include past medical histories and medications, immunizations, laboratory data, radiology reports, vital signs as well as patient demographics (World Health Organization, 2012). The importance of organizational strategy alignment with information systems strategy was emphasized. Functional structuring of business operations in an alignment with information systems strategies can contributes to successful EHR implementation (Eastaugh 2013, Silverman 2013). Developing the strategy integrating the IT systems, platforms with the hospital organization is essential to successful EHR implementation (Silverman, 2013).

**Related Works, Direction of EA and Digital Healthcare**

In the past 10 years, EA has become an important method for modeling the relationship between the overall image of corporate and individual systems. In ISO/IEC/IEEE42010:2011, an architecture framework is defined as “conventions, principles, and practices for the description of architecture established within a specific domain of application and/or community of stakeholders (Garnier et al. 2014).” In addition, EA visualizes the current corporate IT environment and business landscape to promote a desirable future IT model (Buckl et al. 2010). EA is an essential element of corporate IT planning and offers benefits to companies, such as coordination between business and IT, enhancement in organizational communication, and reduction in the complexity of IT (Tamm et al. 2011).

Besides, the EA integration with service-oriented architecture (SOA) that was discussed earlier (Chen et al. 2014), the SOA architecture pattern defines the four basic forms of business service, enterprise service, application service, and infrastructure service (Richards, 2015). The OASIS, a public standards group (MacKenzie et al. 2006), introduces an SOA reference model. Many organizations have invested in SOA as an approach to manage rapid change (Chen et al. 2014). Meanwhile, attention has been focused on microservice architecture, which allows rapid adoption of new technologies like mobile IT applications, cloud computing (Newman 2015). SOA and microservice vary greatly from the viewpoint of service characteristics (Richards, 2015). Microservice is an approach for dispersed systems defined from the two basic forms of functional services through an application programming interface (API) layer, infrastructure services (Newman, 2015). Multiple Microservices cooperating to function together enable implementation as Mobile IT applications (Familiar 2015).

In terms of cloud computing, many mobile IT applications operate with software as a service (SaaS) cloud-based software (Muhammad and Khan 2015). Traditional EA approaches require months to
develop an EA to achieve a cloud adoption strategy, and organizations will demand adaptive EA to iteratively develop and manage an EA for cloud technologies (Gill et al. 2014). Moreover, few studies discussed EA integration with Mobile IT (Masuda, Yamamoto et al. 2018).

Moreover, according to the previous survey research (Masuda, Shirasaka, Yamamoto 2016), when promoting cloud, mobile IT in a strategic manner, a company that has applied TOGAF or federal enterprise architecture framework (FEAF) can adopt the integrated framework using the adaptive EA framework supporting elements of cloud computing.

- **Cloud Computing Architecture**— The NIST cloud computing definition emphasizes three cloud service models: SaaS, platform as a service (PaaS), and infrastructure as a service (IaaS). PaaS is an IaaS platform that includes both system software and an integrated development environment. SaaS is a software application that is developed, implemented, and operated on a PaaS foundation. The SaaS interface is accessed through the client and API interface. IaaS accommodates PaaS and SaaS by offering infrastructure resources such as computing network storage memory through specific centers (Gill, 2015). From standpoints of EA for cloud computing, there should be an adaptive EA framework that is supporting elements of cloud computing (Masuda et al. 2016).

- **Big Data and Digital Healthcare with EHR**— In terms of big data, new computing trends require data with far greater volume, velocity, and variety than ever before. Big data is utilized in ingenious methods to predict customer buying behaviors, detect fraud and waste, analyze product opinion, and react quickly to changes in business conditions (a driving force behind new business opportunities) (Chappelle 2013). The term “big data” refers to data that is so large, it is difficult to process using currently-available IT systems. There is a growing opportunity for analysis, visualization, and distributed processing software to enable users to extract useful information from such data (Boardman et al. 2015). Sources of big data include the following.
  - Corporate data in SQL databases, data in cloud-based SQL or NoSQL databases
  - Data provided by social networks, data provided by sensors in the internet-of-things (IoT)

Big data applications include visualization functionality for effective user presentation of analytical results. Furthermore, big data applications leverage web services that make the results of their analyses available to other applications through APIs; objects in the IoT can be data generators (Boardman et al. 2015). The implementation of big-data analytics in the healthcare field is the process of examining the large data sets involving EHRs to reveal hidden patterns, unknown correlations and other useful information (Chawia et al. 2013; Archenaa and Anita, 2015).

- **Adaptive Integrated Digital Architecture Framework Aligned with Digital IT Strategy**— Our previous research suggested that corporate entities defining digital IT strategies with implementing EA by applying frameworks, such as TOGAF and FEAF, could adopt a framework integrating an adaptive EA framework to provide further support for cloud elements (Masuda, Shirasaka, Yamamoto 2016). Accordingly, another preliminary research of this paper proposed an Adaptive Integrated EA framework depicted in Figure 1 of this preliminary research paper, which should meet with IT strategy promoting cloud, mobile IT, digital IT, and verified this in the case study (Masuda, Yamamoto et al. 2017). The proposed model is an EA framework integrating an adaptive EA cycle with TOGAF or a simple EA framework for different business units in the upper part of the diagram in (Masuda, Yamamoto et al. 2017). The author of the previous paper mentioned above named this EA framework as “Adaptive Integrated Digital Architecture Framework (AIDAF) (Masuda, Yamamoto et al. 2018).”

In the adaptive EA cycle, project plan documents including architecture for new digital IT projects should be made on a short-term basis. This begins with the context phase where project leaders develop above documents by referring to materials of the defining phase (e.g., architectural guidelines for security and digital IT, aligned with IT strategy) per business needs. During the assessment, architecture review phase, the architecture board (AB) reviews the architecture in the initiation documents for the IT project. In the rationalization phase, the stakeholders and AB decide upon replaced or decommissioned systems by the proposed new information systems. In the realization phase, the project team begins to implement the new IT project after deliberating issues and action items (Masuda et al. 2017,2018).
In the adaptive EA cycle, corporations can adopt an EA framework such as TOGAF, etc. based on an operational division unit in the top part of the Figure 1 of (Masuda, Yamamoto et al. 2017) in alignment between EA guiding principles and each division’s ones, which can correspond to differing strategies in business divisions in the mid-long-term (Masuda et al. 2017).

Inhibitors to EHRs Adoption and Implementation

The implementation of EHRs can provide positive performance factor benefits to health care providers, however, there are obstacles hampering the process (Boonstra et al., 2014). There are obstacles to implementation, such as lack of funding and interoperability of current systems, which decelerate the adoption of EHRs (Devkota and Devkota, 2013). There is little evidence in Australian government’s efforts to address the need for interoperability with EHRs through procurement processes. The majority of medical devices, EHRs and other IT systems lack interoperability (Commonwealth of Australia 2017). Along with concern for safety, there are other mitigating factors such as political and economic issues hindering the progress of EHR adoption in the United States (Otto and Nevo, 2013). Furthermore, the greatest obstacles perceived by both adopters and nonadopters involved purchase cost and productivity (Jamoom et al., 2014; Otto and Nevo, 2013). According to nurses and physicians, flexibility of the interface was the factor of highest importance for EHR adoption (Struik et al. 2014). Systems and equipment typically are purchased from different manufacturers, while each comes with its own proprietary interface technology (Commonwealth of Australia 2017). It is also argued that organizational issues had relationships with lack of implementation strategies (Cresswell et al. 2013).

From standpoints of barriers to EHRs implementation, there are needs to consider factors concerning protections and security of patient data even in US, where ARRA expanding HIPPA was passed to protect patients’ records in Congress (Turk, 2015). Across diverse health care settings all over the world, there are concerns from both patients and the public about security and privacy of their EHR information (Papoutsi et al. 2015). Furthermore, interoperable information systems in the health care industry are uncommon and appears to be one of the most frequently referred problems with health care IT (Slight et al., 2015), despite the existence of HL7 Fast Healthcare Interoperability Resources (FHIR) as interoperability standard. Interoperability in cases of hospital EHRs is an inhibitor to implementation (Kruse et al., 2014).

Research Methodology

In this paper, the authors first state research questions to understand the practices and effectiveness of the Governance for EHR using AIDAF in the era of digital IT. Then, the authors evaluate these research questions using a case study, interviews in the government and hospitals in Asia pacific countries such as Australia, Japan, and the United States region. The following research questions should be evaluated in the case of Australian government, reports worldwide, etc.

RQ1: How can digital IT systems in hospitals and government be aligned with digital governance strategy for EHR using AIDAF?

RQ2: How can be EHR improved toward the era of digital IT with AIDAF?

RQ3: How can be EHR managed and organized with AIDAF, involving EHR readiness across countries?

To investigate practices and effectiveness of the governance for EHR using AIDAF, the authors will look into literature reviews and industry trends, the case study in a government and hospitals, where we will build and implement the “AIDAF” and started the operations there.

Then, the authors propose a governance framework for EHRs using AIDAF as hypothesis.

Next, this proposed governance framework for EHRs using AIDAF should be discussed for the analysis and verification in the case study of the government and hospitals using AIDAF in each region. Based on the above research, the authors suggest the effective practices, critical success factors of this proposed governance framework for EHRs using AIDAF for EA practitioners, and refer to the future research.
The Case of Using AIDAF to Improve EHR

Figure 1 illustrates the AIDAF proposed model in the government and hospitals in each region, as the case of applying AIDAF across the healthcare community to improve EHRs. The government in each region, such as US, Australia, implements FEAF based EA basically. EHRs can be defined as one of important elements in the target data architecture in the government. Each principle and target architecture in the government should be referred in the defining phase (architecture guidelines) and assessment, architecture review’s phase (evaluation criteria). AIDAF begins with the context phase. It references the defining phase (i.e., architecture design guidelines related to digital IT aligned with IT strategy covering EHRs in the above government and hospitals in each region), in the structure of digital governance. During the assessment and architecture review, the AB should review the initiation documents and related architectures for the IT project in the above government and hospitals in each region.

As a result of investigating tasks of architecture reviews in the AB, in this case, we confirmed that project planning documents of almost all new IT projects have been submitted to the AB. This board performs an architecture review on the basis of the evaluation criteria and issued the action items there. The reviewers find out the risks connected to each action item and define an equivalent solution for each risk, and Project Management Office (PMO) members can start the risk management process with the AB based on proper mitigation strategy. As this risk management approach, the "STrategic Risk Mitigation Model (STRMM) for Digital Transformation" is shown in Fig 2 as below (Masuda et al. 2017).

The Proposal of Governance Framework for EHR with AIDAF

For the purpose of overcoming the inhibitors to “EHRs adoption and implementation” highlighted in the previous section of “Inhibitors to EHRs” above, the outcome of this research can be divided into four parts. Firstly, funding, economic and political issues to EHR adoption will be identified. This will be addressed by procurement processes in the strategic alignment with the adaptive EA cycle in AIDAF and program governance, while considering a combination of literature review, the above case study and interviews with professionals in this industry. Secondly, concerns about security and privacy of the EHRs’ information and implementation will appear. These concerns will be coped with by risk management model named “STRMM model” in AIDAF (Masuda, Yamamoto et al. 2017, 2018) and security governance. Thirdly,
issues regarding lack of interface, implementation strategies will be obvious. These issues will be addressed by architecture conformance, quality improvement with architecture reviews of adaptive EA cycle by “Assessment model” in AIDAF (Masuda, Yamamoto et al. 2018). Fourthly, issues to EHR adoption and implementation regarding lack of architecture conformance will be coped with architecture reviews of adaptive EA cycle in AIDAF and data governance. Therefore, the authors propose an initial version of governance framework for EHR using AIDAF as shown in Figure 3 below. This framework can be considered as an extension of the AIDAF and IT governance framework like ISO38500, COBIT, etc. These IT governance frameworks will contribute to this proposed framework as the part of “Governance” in Fig 3. The main concept of this proposed framework is that EHRs aligned with IT systems in the government and hospitals can be governed and managed with AIDAF and related appropriate governance frameworks while the AIDAF should directly impact to “Governance” in Fig 3.

Hence, there will be three main elements, “EHR,” “AIDAF” and “Governance” in this proposed framework. These three elements can surround “IT systems in government” and “IT systems in hospitals” in this proposed framework, while EHRs and the aligned IT systems in government and hospitals can be managed and governed with “AIDAF” and “Governance” toward a digital IT era, as shown in Figure 3. The inhibitors to EHRs described in the previous section of “Inhibitors to EHRs” will be addressed in those sets of the above elements, which will be detailed as research progresses.

**Results**

**The Case of PCEHR in Australian Government**

In Australian government, the Personally Controlled Electronic Health Record (PCEHR) system has been architected and implemented in Health Agency by 2012. eHealth is important to the future of healthcare in Australia and is an integral part of the Australian government’s strategy. The agenda for Health Reform is aiming to develop a continuously improving healthcare system for the 21st century. The PCEHR system enables the secure sharing of health information among healthcare providers, while enabling the individual to control who can access their PCEHR. The PCEHR provides global access controls, set of Medicare and healthcare record for patients, sets of PCEHR clinical documents in hospitals and a consolidated view created from these data. The PCEHR system is designed to interface with a number of existing and new systems (NEHTA 2011). These interfaces include consumer oriented systems, healthcare provider oriented systems, repositories like Medicare data and pharmaceutical data and foundation infrastructure such as Healthcare Identifiers, Clinical Terminology, etc. (NEHTA 2011).

Recently, issues have been actualized in terms of specifications for security, privacy as well as interface standardization among EHR related data, clinical systems in each hospital and provider system in each company in Australia. The real privacy issues have been the vast potential risks for misuse by the 900,000 healthcare workers who can access the system, where ill-thought privacy controls and complex access control might lead to the "secondary use" of the data. As an additional privacy risk, health records can be created without the person’s consent (Stilgherrian 2018). As potential risks, all Australians will
automatically be enrolled into online digital health files unless they opt out. Consequently, EHR’s privacy chief in Australia quit to take responsibility for above security and privacy issues (Ben Grubb 2018).

Practically, the above issues can be coped with by architecture and PMO reviews aligned with security architecture guidelines, aligned with Digital Health strategy, covering the risk management model named "STRMM model" in Fig2, in the AIDAF. That is how RQ1 and RQ2 can be verified especially from standpoints of security and privacy. The above architecture, PMO reviews and “STRMM model” can address conformance with interface standard guides, aligned with Digital Health strategy, with security as well. Therefore, RQ1 and RQ3 can be verified in terms of interface standardization involving security.

For the purpose of supporting IT Governance perspectives for the AIDAF, PMO board proceed with program governance for IT systems in government and hospitals with EHR and security governance for these systems with EHR can be coped with AB and security board as well. Therefore, according to our proposed governance framework (Figure 3), Australian government considers and proceeds to application and implementation of the AIDAF and data governance with EHR.

Digital Government Readiness for EHR across countries

OECD compared and analyzed digital governance readiness for EHR across countries, and they showed this result in terms of “Data governance readiness” and from standpoints of “Technical and operational readiness” in the Figure in OECD report (OECD 2017). According to the data analysis by OECD, although EHR was implemented and released in Australia early in 2011, the level of data governance readiness becomes low because aforementioned issues of security and privacy for EHR occurred in Australia these days. Therefore, Australian government consider the application of the AIDAF for the EHR improvement in the above aspects. On the other hand, USA can become high in the level of “Data governance readiness” and “Technical and operational readiness” for EHR comparatively, rather than Australia (OECD 2017) Furthermore, Finland and Singapore have got to the top level from standpoints of both “Data governance readiness” and “Technical and operational readiness” for EHR, and 10 countries are ready to analyze clinical data for healthcare quality monitoring, while Japan is very low in the above both level because EHR is not started yet (OECD 2017). Thus, RQ3 was verified for EHR readiness across countries as well.

Discussion

Benefits of EHR operation using the proposed governance framework

This paper proposed the “governance framework for EHR with AIDAF” to overcome the inhibitors to “EHRs adoption and implementation” in Digital government. The aforementioned case and analysis can suggest that our proposed governance framework could be expected to introduce the following benefits:

• Reducing Risks for managing EHR with digital health applications— In the AIDAF, the AB can review the solution architecture with EHR for all the new Digital Health application projects. The action items should be issued and connected to the risks there, and an equivalent solution can be defined for each risk. In addition, in the following phases, they monitored the status of each risk capable of reducing the risks for Digital Health applications in the digital government, that can lead to enhancing the service levels, security and privacy for patients and doctors, as great benefits of our proposed governance framework, from standpoints of security governance and data governance, EHR adoption, security and implementation as well.

• Improvement of Solution Architecture Quality— In the context phase of the adaptive EA cycle, in the AIDAF, each project team drafted the project initiation documents of new Digital Health applications with EHR related projects based on hospital stakeholders’ needs. This was achieved by referencing the integration, cloud and security-related architecture guidelines developed in the defining phase in the AIDAF. The government’s architecture teams defined principles conforming to Digital Health strategy elements, and established consistency with architecture patterns covering HL7 FHIR for interoperability standard. Moreover, in the architecture review phase of the adaptive EA cycle in the AIDAF, the AB can review the solution architecture in the initiation documents for all the new Digital Health projects covering EHR to improve the architecture quality. These activities are expected to improve the quality of the solution architecture in each new Digital Health applications in the healthcare community, where patients
can use applications covering their requirement in more secure environments and doctors can also utilize their required applications with keeping privacy and security more, as great benefits of our proposed governance framework, from standpoints of strategic alignment and data governance, EHR interface and interoperability as well.

- **Effective Cost Controls for EHR and related digital health applications**— In the rationalization phase of the adaptive EA cycle, in the AIDAF, the AB recognized “replaced systems” and “unnecessary, eliminable information systems”. This was according to the implementation of these proposed new Digital Health applications with EHR and determined the positioning of the new Digital Health applications. These activities of application rationalization can lead to optimal cost control in consideration of the appropriate “replaced systems” and “decommissioned information systems” in the hospitals, government as benefits of our proposed governance framework, from standpoints of program governance, EHR implementation as well.

**Critical Success Factors, Enablers for EHR operation in Digital Government using the proposed governance framework**

Based on the aforementioned case and analysis for the Digital government covering EHR, we identify the following three critical success factors for EHR operation in digital government using our proposed governance framework. These factors and enablers support the EHR improvement and digital governance aligned with Digital Health strategy in a government, hospitals and healthcare community.

- **Commitments from Top Management**— The implementation of digital governance as well as digital government formulation in the healthcare community is often difficult. Even if the digital government with EHR is implemented, on the basis of our proposed governance framework in the healthcare community with hospitals. Commitment from the CIO and top managements of the government, hospitals and their participation in digital governance are extremely important to achieve EHR implementation and digital government formulation in the healthcare community. Early risk identifications and countermeasures for new Digital Health applications with EHR as a result of participation of the top management (digital government CIO, CISO, COO, etc.) should also be very effective. Particularly, for the “digital Health applications with EHR”-related new project strategic alignment risk, countermeasures through participation of the above top management are effective and strategically important.

- **The Formal Architecture Board across the Architecture Teams and PMO Teams**— The formal AB based on collaborative Digital Governance among the architecture community, PMO community, security community and top management is another critical success factor for achieving Digital Government implementation. This EHR is on the basis of our proposed governance framework in the healthcare community and hospitals. It should be a key element to establish program governance and hold monthly meetings of the formal AB to ensure collaboration between the architecture, PMO and security communities, to perform architecture reviews for new “Digital Health applications with EHR” related projects. Moreover, this collaboration is very important to enable the formal AB to discover risks related to project management, security management and data management at an early stage for EHR and digital Health-related projects.

- **Security Architecture Guidelines, and Other Guidelines**—The robust security architecture, standardized security messaging protocol and related architecture guidelines should be extremely important for EHR and Digital Health applications. For security risks in new “Digital Health applications with EHR” related projects, early security risk identification and countermeasures in the formal AB (appropriate adoptions and implementations of EHR, technology architecture and security architecture) should be effective.

**Conclusion**

This research explains and shows the need for the governance framework to manage EHRs in alignment with related IT systems in government and hospitals. The “governance framework for EHR using AIDAF” has been developed, which proposes a way for managing and governing EHRs aligned to digital IT strategies, IT systems in government and hospitals, with the AIDAF. The application of this framework
can help in managing and governing EHRs in the alignment with IT systems in government and hospitals, while addressing key inhibitors to EHR adoption and implementation. This study is expected to contribute to EHRs improvement toward the era of digital IT, with AIDAF and related governance frameworks, such as like ISO38500 and COBIT.

We verified that the EHR case in a digital government that the “governance framework for EHR using AIDAF” could cope with the emerging issues of security and privacy, interface standardizations in the digital government, which can lead to answers for RQ1, RQ2 and RQ3. Furthermore, we compared and analyzed digital governance readiness for EHR across countries that can contribute to answers for RQ3. The main limitation of this study concerns the scope of the research, which was based on data collected from a single case in one digital government. Another limitation of this study is not to refer to aspects of architecture change management and service deliveries with the AIDAF. Moreover, the scope of this research across countries in terms of digital governance readiness for EHR was also limited by data sources, being mostly reports from the OECD.

We suggest that future research should aims to further analyze the effectiveness of the "governance framework for EHR using AIDAF" for her, digital healthcare applications and service delivery perspectives. Such studies should be conducted across multiple countries in the top levels of digital governance readiness for EHR, such as USA, Singapore and Finland. Future research should also explore how the benefits of digital governance can be extended beyond the EHR to other applications.

REFERENCES


Adaptive Governance on EHR in Digital IT era


