Future Internet **2012**, *4*, 621-645; doi:10.3390/fi4030621

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Review

e-Health Cloud: Opportunities and Challenges

Eman AbuKhousa, Nader Mohamed * and Jameela Al-Jaroodi

Faculty of Information Technology, United Arab Emirates University (UAEU), P.O. Box 17551, Al Ain, UAE; E-Mails: emanak@uaeu.ac.ae (E.A.); jaljaroodi@gmail.com (J.A.-J.)

* Author to whom correspondence should be addressed; E-Mail: nader.m@uaeu.ac.ae; Tel.: +971-3-713-5519; Fax: +971-3-767-2018.

Received: 12 April 2012; in revised form: 5 June 2012 / Accepted: 25 June 2012 / Published: 4 July 2012

Abstract: As the costs of healthcare services rise and healthcare professionals are becoming scarce and hard to find, it is imminent that healthcare organizations consider adopting health information technology (HIT) systems. HIT allows health organizations to streamline many of their processes and provide services in a more efficient and cost-effective manner. The latest technological trends such as Cloud Computing (CC) provide a strong infrastructure and offer a true enabler for HIT services over the Internet. This can be achieved on a pay-as-you-use model of the “e-Health Cloud” to help the healthcare industry cope with current and future demands yet keeping their costs to a minimum. Despite its great potential, HIT as a CC model has not been addressed extensively in the literature. There are no apparent frameworks which clearly encompass all viable schemes and interrelationships between HIT and CC. Therefore, analyzing and comparing the effectiveness of such schemes is important. In this paper we introduce the concept of “e-Health Cloud” highlighting many of its constituents and proposing building an e-health environment and elucidating many of the challenges confronting the success of the e-Health Cloud. We will also discuss different possible solutions to address challenges such as security and privacy.

Keywords: health information technology; Cloud computing; e-Health Cloud; healthcare services; security; privacy

1. Introduction

Planning to utilize the latest technologies in the healthcare industry is an important strategy for many healthcare organizations to enhance healthcare services and reduce operations costs [1–3]. There is a high increase in the demand on healthcare services while the shortages in qualified healthcare professionals such as doctors, nurses and pharmacists form one of the toughest challenges confronting healthcare providers [4,5]. In addition, diseases are becoming more complex and new advancements in technology and research have facilitated the emergence of new and more effective diagnoses and treatment techniques [6]. As a result the logistics behind managing such operations has become more complex and very costly. Furthermore, competition among the healthcare industry has risen [7]. Different healthcare organizations provide different types of services to fit the needs of diverse economic categories and disease levels. The marketplace is very competitive while pressure from regulatory authorities forces weak and non-performing hospitals out of business very quickly. In preserving the wellbeing of humans, any reduction in the numbers of healthcare providers or services cannot be tolerated.

HIT has evolved over the years from departmental solutions to encompass larger solutions at the enterprise level, and from stand alone systems that provide limited and localized solutions to more interconnected ones that provide comprehensive and integrated solutions [8]. The complexity of HIT has also evolved from there being passive and reactive systems to now becoming more interactive and proactive with more focus on the quality of care [9–12]. HIT also benefited from the advancements in technology such as database systems, full redundancy for mission critical systems, as well as the recently emerging Cloud Computing (CC) systems to provide efficient and reliable solutions to support health services. According to Foster *et al.* [13], CC can be defined as “A computing paradigm which is a pool of abstracted, virtualized, dynamically scalable, managing, computing, power storage platforms and services for on demand delivery over the Internet.” Emanating from this fact, CC represents the new leading edge for HIT. Utilizing CC for HIT introduces many opportunities to healthcare service delivery [14]. Cloud owners maintain computing facilities, data storage, and software that facilitate the daily routines and procedures of healthcare operations in a flexible and scalable way through effective service-level-agreements (SLAs) *i.e.*, “pay as you use” contracts.

Some healthcare providers have found an opportunity to shift the burden of managing and maintaining complex HIT to the Cloud or more appropriately to the Cloud service providers [15,16]. Thus, in addition to removing the operational load off the shoulders of the healthcare providers, it also significantly reduces the operational and maintenance costs. CC also opened a window of opportunity for healthcare providers to share part of their data with other stakeholders such as government agencies, health research institutes, authorized private companies such as insurance companies and other hospitals. Sharing patients’ data serves different purposes that contribute to improve the quality of healthcare services. Yet this sharing needs to have strict regulations on who is sharing the data and how well the privacy of the patients is maintained. However, according to Kaletsch *et al.* [17], when dealing with privacy and sharing information several threats are involved. The top threats include social functions where, although users can choose to be anonymous, they could easily and involuntarily expose their identity or personal information. Another threat is the selling of medical information as some personal information may not be obvious enough to be excluded before the sale.

In addition users may not find an explicit list of what was distributed or sold and cannot figure out what information about them was included. Further, there is the threat posed by Web analytics done by third parties who use any data available on the Web for user profiling and targeted advertising. In such case some privacy issues arise as such entities observe and record the users' behaviors and their traffic on the Internet thus violating their privacy.

In this paper, we present an overview of the "e-Health Cloud"—a term used in this paper to indicate "integrated HIT solutions available over the Internet on a pay per use model"—and its potential to improve the quality of healthcare delivery. We discuss various proposals and solutions that contribute to the building of successful e-Health Cloud environments in terms of implementation models, HIT solutions development and applications. We then present a high level description of the major challenges facing the e-Health Cloud infrastructure which could hinder its large scale diffusion. It is obvious that the e-Health Cloud will inherit some of the challenges facing general CC in addition to the ones rising from the special characteristics and requirements of health services applications.

One of the challenges facing the utilization of CC for HIT, and the most important as well, is security and privacy. According to the European Commission [18]: "In all countries, trust in e-health systems by both citizens and professionals has been identified as one of if not the key challenge. Privacy is recognized as the most sensitive aspect of e-health records systems." With this important remark, we highlight and analyze a number of current proposed security and privacy solutions in e-Health Cloud. In particular, current solutions focus on network security, access control policies, and client platform security, while they lack the emphasis on integrity and non-repudiation as well as availability. Although there is a reference security model proposed in [19], the model is still in the vision seat.

The rest of this paper is organized as follows. Section 2 presents an overview of e-Health Cloud concepts and opportunities. Technical and non-technical challenges facing e-Health Cloud are discussed in Section 3. Section 4 discusses some research efforts to solve some e-Health Cloud challenges. Section 5 provides a discussion of different schemes to address security issues in e-Health Cloud. We provide some discussion in Section 6. Finally, we offer our concluding remarks in Section 7.

2. e-Health Cloud Opportunities

Cloud computing is an emerging commercial model that allows organizations to eliminate the need to maintain in-house high-cost hardware, software, and network infrastructures. It also reduces or even eliminates the high-cost of recruiting technical professionals to support and operate the in-house infrastructures and IT solutions. Through the use of virtualization and resource time-sharing, the Cloud offers diverse IT solutions as on-demand services for different organizational needs. It is designed to be flexible and scalable thus allowing clients to increase the capacities of their existing system without investing in new infrastructure components. While CC can significantly reduce IT costs and complexities, it enhances resources utilization and service delivery [20]. Different types of organizations can benefit from CC such as governmental organizations, financial enterprises, online entertainment companies, and healthcare providers. The special type of CC that is used for improving patient care is called e-Health Cloud and it provides opportunities to solve some of the current limitations facing HIT solutions [21]. Before discussing the opportunities of the e-Health Cloud, we will explore the current limitations of current e-health systems, some of which are discussed in [22]:

(a) **High cost of implementing and maintaining HIT:** the cost of HIT requires investments in software, hardware, technical infrastructure, IT professionals, and training. This can result in a considerable cost to healthcare organizations in particular for the medium and small sized entities. HIT implementations can be time consuming and stressful for the already stressed healthcare organizations due to demands on healthcare professionals who have to share project responsibilities with their patient care duties. Finally, HIT requires dedicated teams and proper funding to handle day to day management and maintenance.

(b) **Fragmentation of HIT and insufficient exchange of patient data:** HIT in most cases exists as separate small clinical or administrative systems within different departments of the healthcare provider's organization. Therefore, the patients' data exist in a dispersed state where certain portions of this data are restricted within separate departmental systems, certain clinics or areas of the healthcare organization. Such dispersed pockets of data make it challenging to bring information together and share it across the organization or across different healthcare providers.

(c) **Lack of regulations/laws mandating the use and protection of electronic health care data capture and communication:** currently, there are no well established laws or regulations mandating the electronic capture of patient data in addition to law covering issues of protection and security of this data. For example, there is no general law protecting the privacy of patients and the interchanges of their medical data between countries [23]. The data protection standards and regulations are at different levels across countries; for example, the directive on privacy and electronic communications in Europe [24] protects the personal information of patients while the Health Insurance Portability and Accountability Act (HIPPA) and Subtitle D of the HIT for Economic and Clinical Health (HITECH) Act in the United State [25] enforces privacy and security standards for organizations covered by HIPPA.

(d) **Lack of e-Health Cloud design and development standards:** There are no well established standards available for healthcare providers to use to design and build their systems. This would include definitions of data types, forms and at times frequency of data capture in addition to defining how the data is obtained, stored, used and protected. One of the biggest challenges in the area of e-health standardization is the production of multitudinous e-health standards (e.g., DICOM, ISO/TC 215, HL7, *etc.*) developed by numerous standardization bodies (e.g., NEMA, ISO, *etc.*). Many of these are not interoperable or not directly coordinated with each other at an organizational level. More about existing e-health standards is available in the ITU-T technology Watch Report, 2011 in [26].

Moving to the Cloud-based solutions, it is possible to find better ways to resolve these issues and provide more efficient and cost effective solutions. In addition to providing independent per-healthcare provider solutions, the e-Health Cloud also has the potential to support collaborative work among different healthcare sectors through connecting healthcare applications and integrating their high volume of dynamic and diverse sources of information. Dispersed healthcare professionals and hospitals will be able to establish networks to coordinate and exchange information more efficiently.

These networks will be flexible and scalable in integrating and sharing services and data; all of which help in reducing costs and increasing the effectiveness of the healthcare organization. Collecting patients' data in a central location as the e-Health Cloud results in many benefits:

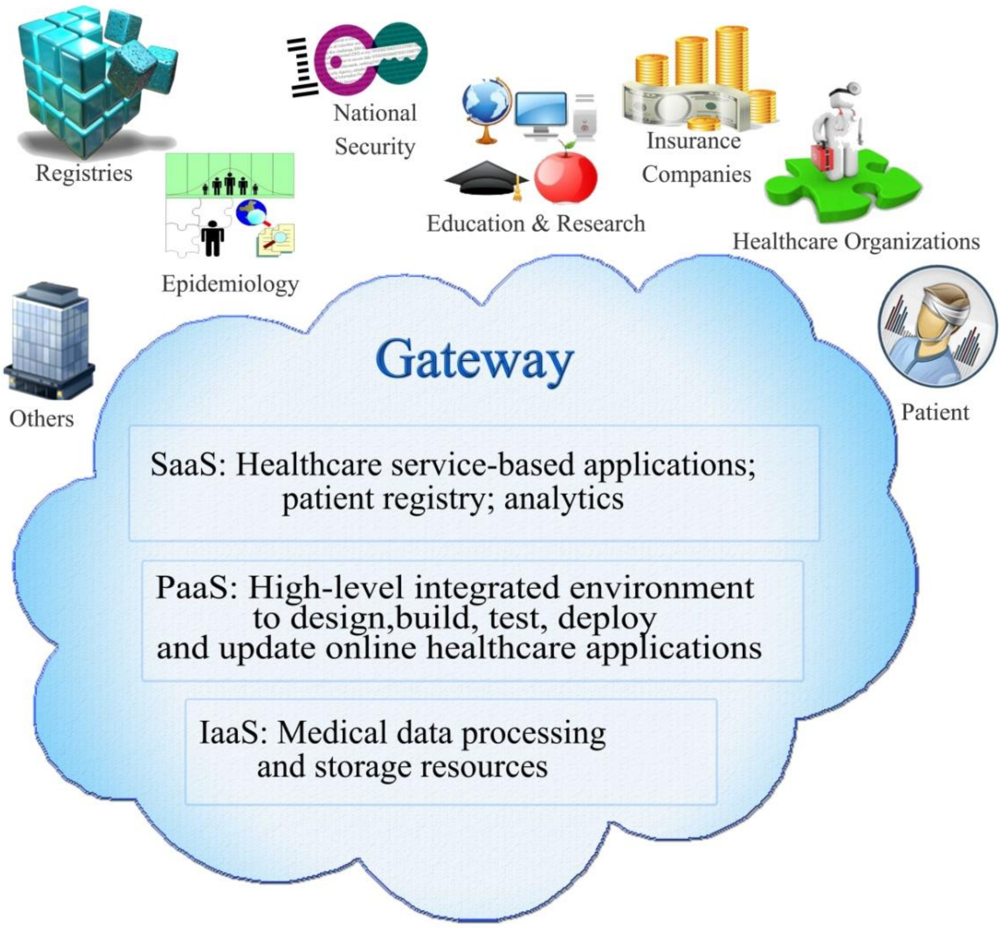
- **Better patient care:** the ability to offer a unified patient medical record containing patient data from all patient encounters across all operators. These records will be available anywhere and anytime allowing healthcare providers to have a comprehensive view of the patient's history and provide the most suitable treatments accordingly.
- **Reduced cost:** the ability to take advantage of the capabilities of CC and create a collaborative economic environment where the overhead costs are shared among the participants; with the flexibility to only pay for actual resource utilization. This feature is very suitable for small and medium sized healthcare providers where they can utilize advanced IT infrastructures and services to support their healthcare operations without facing high initial and operational costs. Another cost reduction aspect is the savings gained from making medical records available globally, thus there are no costs incurred in exchanging and sharing patients' data around the world.
- **Solve the issue of resources scarcity:** the ability to overcome shortages issues in terms of IT infrastructures and health care professionals. This is very important in some areas (such as remote rural communities) with the shortage in primary healthcare facilities [27]. The Cloud enables healthcare providers to use remote medical services and data that help in providing primary healthcare in such areas. It also allows various health care specialists to offer their services remotely thus saving time and effort and reducing the need to have experts available everywhere.
- **Better quality:** the health care operators by having their clinical data stored in the cloud will facilitate supplying concerned entities such as the Ministry of Health or the World Health Organization with information on patient safety and the quality of care provided. The information will be attained by one of two methods; (1) aggregating existing data to arrive at the indicators requested and/or (2) providing on-line ability for health care operators to enter/access data directly. Health care data stored on the Cloud can be aggregated and reported along the lines of generally accepted health care quality indicators such as ones published by the Agency for Healthcare Research and Quality (AHRQ) [28]. AHRQ quality indicators are accepted worldwide and many health care operators use these indicators as measures of performance. For example, the US government will be rewarding US health care operators in 2012 on their ability to meet quality indicators by increasing the payouts they receive from it. This measure was a byproduct of the American Recovery and Reinvestment Act signed by President Barack H. Obama in 2009 [29]. Quality indicators can includes infection rates, lengths of stay and readmission percentages. The other method to collect indicators is for the Cloud owner to provide an on-line tool for health care operators to report incidents such as sentinel events or adverse drug reactions. Such data is important and sometimes it may not be available in the operational data that the operators send to the Cloud, hence creating the need to setup specialized tools to gather it and make it available.

- **Support research:** the e-Health Cloud can offer an integrated platform to host a huge information repository about millions of patients' cases which can be uniformly and globally accessed. This integrated platform can be easily utilized to develop data mining models to discover new medical facts and to conduct medical research to enhance medications, treatments and healthcare services.
- **Support national security:** the e-Health Cloud can increase the ability to monitor the spread of infectious diseases and/or other disease outbreaks. The Cloud can be serviced as an alert system for monitoring the diffusion of any dangerous infectious diseases as well as it can be used to determine the infection areas, the spreading patterns and hopefully the reasons of the outbreaks.
- **Support strategic planning:** decision makers can use the e-Health Cloud data for planning and budgeting for healthcare services. It can also be integrated with other Cloud services to help in forecasting future healthcare services needs. This will help for example in planning the needs for doctors, medical labs and equipments, operating rooms, patient beds, and other medical facilities.
- **Support financial operations:** the ability to streamline financial operations as the Cloud can act as a broker between healthcare providers and healthcare payers. The billing, settlements, and approval processes can be automated and integrated among both parties.
- **Facilitate clinical trials:** the data stored allow the Cloud owner to partner with pharmaceutical companies and medical research institutions for clinical trials for new medicines. As data is collected in an integrated fashion, it is easy to detect the availability of special patients' cases and provide appropriate pools of trial cases.
- **Facilitate forming registries:** the data shared will allow for the formation of specialized registries targeted for specific types of patients such as cancer and diabetes registries.

On the other hand, centralization of health care data on the Cloud may result in a number of risks; though we view these risks as technical and ones that exist with any central store of data scheme. Some of the risks include:

- **Data security risks:** as in accessing patient data by unauthorized users. Many Cloud services offer some security measures. For example, Today's systems in particular HIPAA compliant health care systems—have the ability to record every access attempt by user names and to include date, time as well as relationship to the patient. However, more work is to be done to enhance security and more importantly increase the users' trust levels of these security measures.
- **The risk of loss of data:** Although it is a significant issue, advancements in database management systems such as Oracle, Cache' and SQL have created concepts of hot and cold backups, mirroring and data base restores to provide efficient solutions that minimizes this risk. Not to mention, off site backups and disaster recovery sites.
- **The risk of systems unavailability:** losing an e-Health service could be a major issue especially in an emergency situation. However, advancements in the science of business continuity have increased systems reliability and availability.

Figure 1. The generic architecture of e-Health Cloud.


Registries
National Security
Education & Research
Insurance Companies
Healthcare Organizations
Epidemiology
Others
Patient
Gateway
SaaS: Healthcare service-based applications; patient registry; analytics
PaaS: High-level integrated environment to design,build, test, deploy and update online healthcare applications
IaaS: Medical data processing and storage resources

e-Health Cloud as presented in Figure 1 is a special-focus Cloud that provides IT services to improve patient care while increasing operational efficiency. Typically, the Cloud consists of an array of layered elements, starting at the most basic physical layer of storage and server infrastructure and working up through the application and communication layers. The e-Health Cloud can be further divided into different implementation models based on whether it is created internally (private Cloud), outsourced (public Cloud) or a combination of the two (hybrid Cloud). The layers of e-Health Cloud aim to help optimize the healthcare data facility environment, to create a platform that provides pre-built software tools for specialized HIT providers and software designers; and finally to provide Cloud-based HIT solutions for healthcare providers, patients and other concerned organizations such as insurance companies and research facilities. The e-Health Cloud consists of a Gateway and Service-Based Applications in addition to the generic three-layer architecture of the Cloud:

- **Gateway:** This component can be set to perform several important tasks: (i) managing access to the Cloud; (ii) verifying EHR (Electronic Health Record) provided by different health care providers in terms of integrity, authenticity, confidentiality and compliance with medical data exchange regulations; (iii) combining and integrating EHR data into a new composite Cloud-based EHR; (iv) selecting and de-identifying EHR to share with the public Cloud for research, educational and industrial purposes [22].

- **Service Based Applications:** such as services for national security and epidemiology, registries, Web Portal, Picture Archiving and Communication Systems (PACS); all of which provided as services that are easily managed through CC operational parameters.
- **Software as a Service:** provides Cloud-based software solutions (e.g., clinical systems; CSM) where consumers such as healthcare providers or financial and insurance brokers receive access to the software capabilities of the cloud.
- **Platform as a Service:** extends the basic infrastructure with High-level integrated environment to design, build, test, deploy and update online healthcare applications.
- **Infrastructure as a Service:** physical processing and storage resources.

3. e-Health Cloud Challenges

Although the e-Health Cloud could provide valuable benefits to the health care industry, it unfortunately inherits the major challenges of HIT and CC together and adds more weight to these challenges as it is used to store and process sensitive medical data. Here we summarize the technical [21,30–36] and non-technical [21,31,32,37–41] challenges particularly faced by the e-Heath Cloud.

3.1. Technical Challenges

- **Availability:** Most healthcare providers require high availability of the e-Health Cloud services. Service and data availability is crucial for healthcare providers who cannot effectively operate unless their applications and patients' data are available. The e-Health Cloud services should be available continuously with no interruptions or performance degradation. Cloud services could experience failures due to software and hardware faults, network faults, security attacks, and natural disasters among many other reasons. As CC resources are distributed over an open network such as the Internet, they will not offer better availability compared to owning and maintaining IT infrastructures within the organization [42]. e-Health Cloud environments need to make serious provisions to react rapidly and efficiently to such outages and ensure service continuity to the participating healthcare providers and other organizations. In addition, hardware and software installations, upgrades, and reconfigurations should be managed such that they are done without any service interruptions for the healthcare providers.
- **Data/Service Reliability**: using the cloud for an important application like e-Health Cloud requires assurances of good reliability for the provided services. All e-Health Cloud services and data must be error-free. Some important decisions regarding single human or society health can be taken depending on the data and services provided by the e-Health Cloud. As such services are distributed and may come from a number of Cloud providers, the chance of having faulty or incorrect data or services can increase. The data in e-Health Cloud must be consistent and constantly in a valid state regardless of any software, hardware, or network failures. In addition, all e-Health Cloud must deliver error-free services for healthcare providers.
- **Data Management:** Huge numbers of medical records and images related to millions of people will be stored in e-Health Clouds. The data may be replicated for high reliability and better access at different locations and across large geographic distances. Some of the data could be

also made available locally. Most medical applications require secure, efficient, reliable, and scalable access to the medial records. These requirements enforce the need to have some storage services that provide fault tolerance, secure storage over public clouds, and rich query languages that allow efficient and scalable facilities to retrieve and process the application data.

- **Scalability:** hundreds of healthcare providers with millions of patient records could be handled by an e-Health Cloud, which is only achievable if and only if the services provided are scalable. The ability to scale (grow while maintaining acceptable performance) is one of the most important factors in providing successful cloud services. Cloud scalability is mainly enabled by increasing the capacity and number of IT resources such as compute nodes, network connections, and storage units and providing suitable operational and management facilities. Scalability requires dynamic configuration and reconfiguration as well as an automatic resizing of used virtualized hardware resources [43]. In addition, scalability requires maintaining an acceptable level of performance regardless of the size and utilization levels of the services.
- **Flexibility:** an e-Health Cloud must be capable of serving multiple healthcare providers with different requirements. These requirements are in terms of functions, operations, users, auditing, management, and quality of service (QoS) requirements. The e-Health Cloud infrastructures and services should be flexible enough to be configured for different healthcare providers' requirements. In addition, the e-Health Cloud should be very flexible in adding new needed services to support healthcare processes. While e-Health Cloud services must be flexible to meet different healthcare requirements, they also must be easily configurable to meet with different needs. In other words, the configuration of cloud services to meet different requirements must be achieved with minimum effort and cost.
- **Interoperability:** services for the e-Health Cloud can be provided from multiple cloud service providers. For example, one provider may provide storage and processing services for high resolution medical images while another provider may provide storage and other services for storing patient electronic records or data mining and analysis services. The main issue here is interoperability which involves defining an agreed-upon framework or some open protocols/APIs that enable easy servers and data integration among different cloud service providers [44]. The common framework or protocol should also include mechanisms for secure information exchange and services' integration. The issue of interoperability is also faced when integrated e-Health Cloud services are provided from both local and external clouds. For example, some e-health functions can be developed by integrating some local and external services. These e-Health Cloud services cannot be formed easily unless there is a good degree of interoperability among the local and external service providers. A good degree of interoperability can also facilitate easy migration among different available systems. Data migration between an old local application and a new e-Health Cloud can be simplified if open protocols and APIs are provided. One approach is to utilize the concept of Service-Oriented Architecture (SOA) [45,46] for implementing the e-Health Cloud. SOA aims to make services available and easily accessible through standardized models and protocols without having to worry about the underlying infrastructures, development models or implementation details. This helps achieve interoperability and loose coupling among e-Health Cloud components and also among e-Health Cloud users.

- **Security:** the e-Health Cloud services can be provided by multiple cloud service providers and be used by multiple healthcare providers. The cloud service providers provide a number of recourses that are collected in a virtualized pool to be utilized by healthcare providers. High security concerns are usually associated with open environments which are provided by a number of service providers and shared among a number of service consumers. A healthcare provider that owns IT applications within its premises can apply and monitor proper security policies and controls for identity and access control managements. However with open environments, it is very important to provide cloud services which support suitable and adequate access control and authentication mechanisms in addition to mechanisms to secure the transfer of such data to and from clients and service providers. That is essential since data must be kept secure in the multi-tenant clouds where it is stored along with other healthcare providers' data. In addition, it is necessary to make sure that the service provider itself cannot access or use the healthcare providers' data. Another issue is the need for efficient security mechanisms for the e-Health Cloud. While there are several ways to apply strong security measures, these impose high computation and communication costs rendering them inefficient in distributed open environments such as the Cloud. In addition, another issue is the wide range of security requirements among healthcare providers, thus an organization's security requirements and policies may not be fully reflected in cloud services [47].
- **Privacy**: privacy is an important CC issue that could prevent the full utilization of its capabilities for different types of organizations and applications [48]. Privacy is particularly one of the main concerns in e-Health systems [49,50]. When using the Cloud for e-Health services, this concern is amplified. The concerns here involve the ability to protect patient's records from each other, other healthcare providers and the cloud service providers. In addition, all associated organizations also require certain access to records or parts of records, while trying to protect their own data. Controlling such a maze of interconnected data and entities and using it is a huge issue. Patients, healthcare providers and any other associated organization will worry about the privacy of their information and would like to see proper solutions to offer acceptable privacy levels before moving to the cloud.
- **Maintainability**: Unlike having an e-health system for individual healthcare service providers, an e-Health Cloud can be used for hundreds of healthcare service providers. This increases the complexity of system maintainability in the e-Health Cloud compared to an individual e-health system. The increase is mainly due to the need to consider the requirements and characteristics of the multiple heath services providers and clients. These requirements can be completely different while maintenance in the cloud infrastructures, software, or platforms must be done without having any negative affects on any services provided for any clients. In this regard and to simplify the maintenance processes, all cloud resources and provided services must be designed for easy and reliable maintenance. In addition, testing models can be developed to simplify the process and to reduce the time needed for maintenance.

3.2. Non-Technical Challenges

- **Organizational change:** the move towards e-Health Cloud will require significant changes to clinical and business processes and also to the organizational boundaries in the healthcare industry. This challenge is concerned with the changes that an e-Health Cloud will introduce upon participants. Examples of such changes could be in the form of new policies, procedures and workflows in addition to changes in how medical processes and documentation are done.
- **Legislations and standards:** there are still no clear or adequate legislations and guidelines for clinical, technical and business practices of healthcare in the e-context. This includes the lack of standards for medical informatics, policies, inter-operability, and transmission methods in e-Health Cloud. In such a case, the stakeholders in the e-Health Cloud do not have a solid base to start offering and using it. As a result, more issues and problems may occur due to this shortage and technical, social and ethical concerns will arise. Currently, there are some standards and classifications for health information systems in general some of which can be adopted for the e-Health Cloud. One example is the International Classification of Diseases tenth revision (ICD-10) issued by the World Health Organization (WHO) [51]. It defines a medical classification list for the coding of diseases, signs or abnormal findings, complaints, social conditions, and external causes of injury or diseases. Another classification is The Systematized NOmenclature of MEDicine (SNOMED) which was designed as a detailed categorization of clinical medicine for the purpose of storing and/or retrieving records of clinical care in human and veterinary medicine [52]. The e-Health Cloud developers can agree on adopting some of these defined standards and classifications to enable interoperability among different organizations.
- **Data ownership:** ownership of data in the healthcare industry in general is an area with no clear guidelines. A patient’s record for example could be the sole property of the patient, yet can his physician also claim ownership? What about the patient’s insurer or the hospital management? This challenge is concerned with the creation of policies and guidelines that draw clear ownership boundaries.
- **Privacy, trust and liability issues:** this challenge is concerned with the risks of private data exposure, data leakage, and data loss and the lack of knowledge about the location and jurisdiction of the medical data. From the healthcare providers' perspective, e-Health Cloud presents a high risk of liability (legal responsibility) in cases of data loss or leakage causing loss of reputation and patients’ trust.
- **Usability and end users experiences:** this challenge is concerned with the degree and level of adoption obtained by the e-Health Cloud users including patients, healthcare professionals, and administrative and insurance personnel. Proper and adequate pre-implementation training and marketing along with continuous post-implementation training are important to help overcome this challenge.

Among all the challenges listed above, trust, privacy and security emerge as the major concerns for the e-Health Cloud. Hence, several efforts in this area try to offer solutions to tackle these concerns and improve the security and privacy of the e-Health Cloud.

4. Research Efforts

There are several efforts that introduce contributions to building the environment for e-Health Cloud. We could group these efforts into four categories: (1) Cloud-based storage solutions and HIT applications or systems; (2) platform solutions; (3) e-Health Cloud implementation models; and (4) security solutions for e-Health Cloud. We will discuss solutions in the first three categories in this section, while the fourth category will be discussed in Section 5 due to its significance and importance.

4.1. Cloud-based Storage Solutions, HIT Applications and Systems

There has been some work carried out in designing storage and file management systems for e-Health Cloud. Guo *et al.* [53] proposed a Cloud-based intelligent hospital file management system (HFMS) that aims to improve some of the limitations which characterize the traditional hospital management systems (HMS). Such limitations include limited storage capacity of some of the hardware devices and slow performance of the hardware due to the huge amount of data, the backup models, and the resource sharing across different platforms. The proposed Cloud-based HFMS consists of a master server and multiple blocks of servers. Large files are divided into fixed-sized blocks and each block is backed up by three blocks. The master server manages the file system meta-data that includes namespace, access control, file-block mapping and physical address of relevant information. This model is claimed to adopt low-cost server clusters with the flexibility to allow the applications to overcome the physical boundaries, maximizing the utilization of total systems resources as needed.

Chen *et al.* [54] proposed to store patients' data in the Cloud to meet the growing demands of storage space for EMR and at the same time to fulfill the significant requirements for data security and privacy protection. The proposed method suggests storing distributed EMR at a local storage system and other two different commercial clouds using the algorithm of RAID 3 (redundant array of inexpensive/independent disks). Using RAID 3, the segmented data stored in each Cloud will be meaningless and useless. To ensure the integrity of data upload and download, a cryptographic hash function (MD5: Message-Digest algorithm 5) is used in association with RAID-3.

Teng *et al.* [15] provided a long term off-site medical image archive solution for digital imaging and communication in medicine (DICOM). One of the biggest challenges which the healthcare industry struggles with, is the growing cost of managing long-term onsite medical imaging archives. The continually increasing need for high volumes of medical images is resulting in scalability and maintenance issues with picture archiving and communication systems (PACS). The tools and functionalities of the Windows Azure Cloud platform were used to develop and deploy the prototype of DICOM image archive service. The prototype system was tested with a variety of public domain DICOM images. The tested image series were successfully sent from clients, received and indexed by the server in the Cloud, retrieved as requested in queries and returned. With the rich features and supports of Azure, the system has the potential to reduce the cost of image archives storage and management and to enhance the disaster recovery capabilities.

In addition, Rolim *et al.* [55] proposed a solution to automate the process of patients' critical data collection, distribution and processing. This is to reduce manual efforts, eliminate typing errors, and improve patients' data accessibility. The proposed automatic solution uses a network of sensors connected to legacy medical devices to collect patients' vital data and deliver it to the e-Health Cloud for storage, processing, and distribution. Finally, a group developed a cloud-based Early Warning Service (EWS) [56] that enables the simulation of patients' data. EWS has the potential of fully automating the process of calculating the patient's risk index by capturing vital signs using medical sensors, transmitting the captured values to data buckets in the Cloud, constantly monitoring the patient's status, and notifying clinicians by calling or messaging their mobile phones when necessary.

4.2. Platform Solutions

There have been some efforts to investigate using the current general commercial Cloud platforms for e-health services. In addition, there have been other efforts to propose new Cloud platforms that are specifically designed for e-Health services. White [57] provided an insightful discussion of advantages and disadvantages of using commercial platforms and Clouds (such as Windows Azure, Google Apps) by healthcare organizations for their e-Health Cloud applications. For example the benefits of fast and low cost implementations are a tradeoff with the security risks and outage issues of the Cloud providers.

On the other hand, specialized e-Health Cloud platforms can provide a set of common services specifically needed for developing and operating different e-health applications. In one example, Fan *et al.* [58] presented the Data Capture and Auto Identification Reference (DACAR). DACAR aims to develop, implement and disseminate a novel secure platform in the Cloud for capturing, storing and consuming data within a healthcare domain. By using a single point of contact, the DACAR platform promises to provide solutions for the challenges of e-Health Cloud services. This is done through a rule based information security policy syntax and data buckets hosted by cost effective and scalable cloud infrastructures. These services include integration, large scale deployment, security and confidentiality of medical data. The DACAR platform was also used to develop EWS software [56] and it is the only platform so far that is designed specifically for e-health services.

In another specialized e-Health Cloud platform example, researchers developed an approach for a cloud platform called CyberHealth for Aggregation, Research, and Evaluation (CARE) [59]. This platform was mainly proposed to enable data integration, filtering, and processing for data mining in e-health. They identified a need for an infrastructure for data integration and languages, algorithms, and tools to analyze medical information to discover new medical patterns. With this approach, heterogeneous data from different sources can be integrated, processed and analyzed to improve health understanding and medical treatment effectiveness.

Generally, general cloud platforms can be more open to integration with other applications, while specialized e-health platforms can provide better customized environments for implementing, integrating, and operating e-health applications.

4.3. e-Health Cloud Implementation Models

Some efforts were invested in the e-Health Cloud implementation models. One example is a practical e-Health Cloud implementation model to support the construction of HIS for small healthcare providers who cannot afford to have their own HIS systems [60]. This solution imposes uniform standards of data sharing between existing HIS. The model suggests using a virtual private network (VPN) with the support of public networks such as the Internet to establish a private Cloud through which different hospitals can share HIS information. The VPN framework is easily implemented by adding a secure communication model to the existing HIS systems. This secure communication is used to connect to the Cloud for data transmission, storage and sharing.

Another example is the introduction of the concept of shared and scalable infrastructure for e-Health Cloud across public and private networks [16]. The paper claims that to gain full leverage of the possibilities of offerings of the three layers in different private and public clouds, healthcare organizations will need to develop disciplined internal private clouds. These private clouds will, as technology evolves, exploit secure network techniques and virtualization tools to seamlessly merge locally hosted applications and services with those provided on the public Cloud, or the Internet, as well as those provided on private Clouds.

Yu [61] investigates utilizing a service modeling approach to model the requirements and design of different Service-Oriented Architecture (SOA) based services by using Service Oriented Modeling and Architecture (SOMA) and employing Service Oriented Modeling Framework (SOMF) modeling styles and assets. SOMF is a service oriented modeling language which serves as a tool for developing diverse service oriented models. The paper demonstrated the steps of building an SOA based healthcare application using SOM architecture and SOMF service modeling for handling the application requirements. It shows how to rapidly implement and evaluate e-health applications using this approach. Generally SOA can provide a good solution for facing some of the development and operation challenges facing the e-Health Cloud.

5. Security and Privacy Challenges in e-Health Cloud

Security and privacy in the e-health and other domains are generally the same issues mostly raised as the Cloud clients look to move their data and applications to the Cloud [62]. Security and privacy protection of patients' records in the e-Health Cloud is of absolute importance and involves various requirements. First, the creation and maintenance of cloud-based healthcare e-records of any type should preserve content authenticity, integrity and privacy. Next, all healthcare data should be guarded in secure storage with protective access mechanisms and secure transmissions. Last but not least, the access and sharing of healthcare data should provide an end-to-end source verification, confidentiality and auditing capabilities. Thus, the common security and privacy issues in the e-Health Cloud include:

- **Confidentiality:** ensuring that healthcare data is not accessed by unauthorized parties.
- **Integrity:** ensuring the accuracy and consistency of healthcare data.
- **Authentication:** ensuring that users are the persons they claim to be.
- **Access control**: ensuring that users access only healthcare data that they are allowed to access based on their authentication and access levels.
- **Non-repudiation:** ensuring that a party of a communication cannot deny having sent or received the data.
- **Privacy:** ensuring that patients maintain the right to control what healthcare data is collected about them, how it is used, who uses it, who maintains it, and what purpose it is used for.
- **Audit:** ensuring the safety of healthcare data and the e-Health Cloud overall system by recording and monitoring all users and data access activities.

Research on the security issues surrounding e-Health Cloud has been growing fast over the last few years. The security in the context of the Cloud has a complex maze of issues that must be addressed. However according to Grobauer *et al.* [63] we should make a clear distinction between technical security risks facing any IT infrastructure and those risks imposed solely due to the nature of the Cloud. Risks arising from the specific characteristics of Cloud Computing, related to specific innovations in the cloud, prevalent to the intrinsic core cloud technology or state-of-the-art cloud offerings. As a result, when analyzing the security risks for the e-Health Cloud, it is similarly important to try to separate the different types of risks to simplify the process of incorporating adequate security measures. However, as we will see in the following examples, most approaches handle the problem as a holistic approach and try to resolve all issues at once. Here we present some security solutions and approaches that have been proposed to fulfill the requirements for securing the storage and providing access controls of healthcare data in the Cloud.

One approach suggested that the best way to deal with the risks of privacy exposure is to allow patients who are PHR owners to have full control over the selective sharing of their PHR data [64]. So instead of the Cloud owner encrypting the patients' data, patients can generate their own decryption keys utilizing attribute-base encryption (ABE) and then distribute them to their authorized users. Patients will be able to choose in a fine-grained way which users can have access and to which parts of their PHR by encrypting the record according to a relevant set of attributes. Patients also maintain the right to revoke access privileges when they want to. This model creates a patient-centric PHR system within which multiple owners encrypt data according to their own ways using different sets of cryptographic keys. The approach also proposes a flexible data access policy that allows changes especially in emergency cases within which the regular access control policies could be broken to allow a type of “break-glass access to PHR.” However, apart from the computation overhead on the patients for key distribution and data or user management, this approach does not address the risks of privacy exposure by the Cloud owner.

Some methods can be devised to resolve the challenge of heavy computation attached to the previous structure within which the owner is required to carry all the operations of data and user management in addition to the tasks of re-encryption in case of user revocation and at the same time to protect data privacy against cloud owners. One way to do that is by allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to the cloud owner without disclosing the original data content [65]. This can be accomplished through utilizing combined advanced cryptographic techniques: Key-Policy Attribute-Based Encryption (KP-ABE), Proxy Re-Encryption (PRE) and lazy re-encryption. Each record is associated with a set of attributes and each user is assigned an expressive access structure that is defined over these attributes. To enforce the attribute-based access control, KP-ABE is used to guide data encryption keys of data record. PRE is combined with KP-ABE to enable the data owner to delegate most of the computation operations to the cloud owner but without disclosing the underlying record contents. By this, data privacy is maintained as the cloud owner is not able to decipher any “plaintext medical data.” In this approach, scalability is also achieved using a lazy re-encryption technique to allow cloud owners to “aggregate” the computation tasks of multiple system operations. This causes the computation complexity to be either “proportional to the number of system attributes”, or “linear to the size of the user access tree”, which is independent of the number of users in the system. However, this approach does not address the need for data access policies management and the mechanism to serve emergency scenarios.

Moreover, in [66] the authors argue that forensic methods are the best to use to ensure privacy, confidentiality and tracking of activities at the Cloud owner end of the e-Health Cloud infrastructure. The approach proposes computer forensic tools (CFT) as an acceptable security model for health records over the Cloud. It involves installing data loggers and sniffers on the cloud machines to capture any volatile information. At the same time, nonvolatile information has to be protected through different authentication, authorization and access control mechanisms. The approach also recommends supporting the e-Health Cloud architecture with legal mechanisms and periodic certification by a Third Party Audit (TPA). The forensic and anti-forensic tools and studies are performed by TPA to dynamically check the activities of the Cloud owners. Although e-Health Cloud with CFT has the potential to earn the clients' confidence; the approach watches and reports the volatile actions, but it does not physically prevent them from happing in the first place.

From a different angle, [21] provides a technical solution to particularly address the security issues of end-user platforms and external storage. End users do not use their platform to only access health records in the Cloud but also for other applications. Therefore, and with the limitations of security features within operating systems, end users platforms become very vulnerable to malware attacks which can obtain the user's passwords and secret data. This is in addition to the issue of transferring medical data to mobile storage units which take them away from any security control in the Cloud. To address all these issues, this approach proposes constructing trusted privacy domains (TVD) for the patients' medical data. Systems in the end-user platform should be able to divide the execution environment for applications into separated domains isolated from each other. Medical data is kept within TVD that is accessed only by authorized users. Data leakage can be prevented by the TVD infrastructure and security architecture. When medical data is stored on external storages, the system automatically encrypts the data with a key that is only accessible in the corresponding privacy domain. While when exporting data to external systems that are not connected to the TVD, a security gateway is introduced to control the data export under a data protection protocol.

A key feature of the TVD infrastructure is its automatic management. The TVD establishment, key management and policy enforcement are totally transparent to the users. The infrastructure automatically verifies the integrity of client platforms when they try to join a TVD and then distributes keys and policies. Policy enforcement and data encryption are handled by a security kernel in the client platform without any kind of user interaction. The connection is secured between different platforms using an IPSec-secured virtual private network. Nevertheless, the approach entails that the end user platforms contain a security hardware module such as the Trusted Platform Module (TPM). However, this cannot be the case for all devices especially those used by patients. On the other hand, a privacy domain is established in the Cloud and enforced on the client platforms of the healthcare providers for each application which raises concerns about the complexity and scalability of this approach.

In another approach, Kaletsch and Sunyaev in [17] introduced a privacy framework to support EHR exchange by allowing general practitioners to securely transfer information to specialists through the online referral and appointment planer (ORAP). In ORAP security model, EHR is only stored at the physicians' practices, which are considered to be the only trusted environments. EHRs are encrypted and signed before leaving the physician's practice to the central or cloud storage and they can only be decrypted by the receiving specialist. The patient's home, also, is not considered to be a secure environment and so patients cannot access the EHR from their homes. At the current stage, the ORAP model does not secure any patient-centric functions (e.g., medical history, action plan, collaboration tools) nor enable users to work with single EHRs entries (e.g., view, update). The model just allows transferring EHR securely when a referral is made.

Finally, the DACAR platform for e-Health Cloud [58] was developed with the most common requirements for security such as: (a) cryptographic protocols to verify identities; (b) individual and role-based policies to control and provide access rights to resources; (c) functions to ensure that during any operation, data is accurate, complete and consistent; (d) mechanisms to protect data from any unauthorized disclosure by assuring that stored or transmitted data are accessible only to those authorized to have access; (e) mechanisms to keep track of a chronological sequence of audit records. Examples of security techniques incorporated in DACAR are digital signature, hashing and encryption, integrity check-sum, Single Point of Contact (SPoC), access controls, audit trail and identity mapping.

Obviously, the current solutions for e-Health Cloud security which may include access control and data encryption would require the development of management policies, users' privileges, authenticity certificates and cryptographic keys. Many solutions revolve around patient-centric solutions as they provide patients with better control over their content and more trust in the system as they know they have the final say on who accesses their data and how. However, this approach has some drawbacks and the most important of which is the increased responsibilities of the patients. A patient needs to be aware of the process of protecting and disseminating his medical records which would be very hard for a significant percentage of users. In addition, the overhead imposed on the patient's processes is high and may cause problems. Furthermore, the issue of emergency access does not have a clear and feasible solution. What happens if the patient is not available to grant access? What if he/she is in a serious condition and cannot respond? These questions require more work to be done to enhance this model. On the other hand, delegating the responsibilities to the service provider may relieve the patient of this burden, yet it will increase the issues of trust and control as the patient in this case cannot control the privacy of his/her data. In addition, handling multiple patients' records imposes more overhead on the provider and complicates policy handling. Later on, we could move the responsibility to the cloud owners; however, we risk further exposure and cannot have strong guarantees to the patient about the privacy of his/her data. In addition having to handle multiple service providers each with many patients will increase the overhead and complexity of deploying specific privacy policies for each one of them. As a result, more work is needed in this area to come up with more flexible, less complex solutions to ensure the security and privacy of medical records. One possibility is to distribute the responsibilities among all stake holders and provide methods to localize parts of the process at each level. Patients, service providers and cloud owners must collaborate to provide a solution that is acceptable to all parties. Table 1 provides a summary of the security approaches we discussed above and how they offer some of the security features. Such solutions are hampered by a number of challenges that emanate mainly from various complicated clinical, administrative and financial workflows in the healthcare process, and also to the type of "life critical" medical data. For example, what if an authorized person is unable to access the system due to any reason? The system must ensure that a correct way is devised to access medical data in case of an emergency where the patient is not available to access the data to avoid endangering the patient's life. Another issue that may arise is what if the owners of the patient records decide to delete a record? How will the patient be assured that no data is left in the Cloud? What about the patient's safety in this case? This is a crucial issue because security is still one of the key deterrents that prevent many healthcare organizations from adopting e-Health Cloud solutions.

Table 1. Summary of various proposed security approaches.

Work	Objective	Approach	Advantages	Limitations
[64]	Secure personal health record (PHR).	Patient-Centric and fine-grained data access control through multiple-owner settings model.	Fine-grained access; user revocation; flexible data access policy; beak-glass access.	Computation overhead on data owner; risks of privacy exposure by cloud owner.
[65]	Secure PHR, maintain data confidentiality against cloud owner; reduce overhead on the data owner for key distribution and data/user management.	Allow data owner to delegate computation tasks in fine-grained data access control to cloud owners without disclosing content by combined advanced cryptographic techniques: Key-Policy Attribute- Based Encryption (KP-ABE), Proxy Re-Encryption (PRE) and lazy re-encryption.	Cloud owner is not able to learn any "plaintext medical data"; computation overhead is reduced on users which saves their efforts and time online; scalability.	Limited data access policies management; no mechanisms to serve emergency scenarios.
[66]	Ensure privacy and confidentially of EHR; Track activities at the Cloud owner end of the e-Health Cloud infrastructure.	Install Computer forensic tools on the cloud machines to capture any volatile information. Different mechanisms of authentication, authorization and access control procedures to protect nonvolatile information.	Protect medical data confidentially against cloud owners; CFT provides digital evidence to be used to establish cyber crime in courts of law.	CFT promises to track volatile actions and to support cases in courts; but it does not physically stop volatile actions.
[21]	Secure end user platforms when accessing e-Health Cloud.	Trusted privacy domains (TVD): Systems in the end-user platform should be able to divide the execution environment for applications into separated domains isolated from each other.	Overcome limitations of security features within end user platforms; reduce security risks; Automatic management (transparent TVD establishment, key management and policy enforcement).	Hardware requirements; complexity and scalability
[17]	Secure EHR exchange when a referral is made.	EHR is only stored at the physicians' practices (the only trusted environment). EHRs are encrypted and signed before leaving the physician's practice and decrypted only by the receiving specialist.	Provides secure encryption and signatures for all documents transferred.	Patient and patient-centric functions are not integrated in the current model.
[58]	Develop and disseminate specialized secure services/platforms for e-Health Cloud.	Digital signature, hashing and encryption, integrity check-sum, Single Point of Contact (SPoC), access control, audit trial, identity mapping, *etc.*	A complete e-Health Cloud services platform, provides mechanisms to reinforce medical data confidentiality, security, integrity & auditing.	Comprehensive evaluation in a real medical environment; Integration with other public e-Health Clouds.

6. Discussion

It is evident that the e-Health Cloud presents promising opportunities for the healthcare industry which is still facing serious challenges. These challenges include patient care quality and safety, dramatically increasing healthcare costs, hardware costs and limitations, computing and access speeds, backup capabilities, security, resources scarcity; and most importantly, collaboration and knowledge sharing among healthcare professionals at local and international levels. As a result, the e-Health Cloud could be viewed as a suitable method to provide a potential solution to the value equation in the healthcare industry: "high quality services at the lowest cost."

Adopting the e-Health Cloud to provide IT solutions for the healthcare industry comes with many advantages. Some of these include

1. Reducing the cost of owning and maintaining an IT infrastructure and support personnel within each organization.
2. Providing better integration and exchange of medical records across multiple organizations and across sparse geographical areas.
3. Allowing multiple parties to benefit from the information repository to streamline processes, enhance diagnosis, support medical research activities, and simplify administrative operations.
4. Increasing the availability, scalability and flexibility of the health information systems.

However, these benefits come with a high tax. Several issues and challenges need to be addressed before the e-Health Cloud is considered the best approach to take for healthcare providers. The major concern is security and privacy issues. To date, the available security and privacy measures offer some level of confidence, yet they also involve high overheads and many weaknesses and loopholes. Issues of ownership and control over the security policies involve very complex tasks that need to be taken care of by several of the e-Health Cloud participants. However, the simple task of deciding who is responsible for which part is difficult and has no clear way of being done. In addition, if we include strong security measures, we also risk being in critical situations where someone must have access to some protected data when the owner is not available. One simple example is when a patient who is the only one who can release his/her medical records is involved in a severe accident and he/she becomes unable to release the records. In such case, is it possible/acceptable to have a back door for the records? Who should be responsible for such a task? On what grounds, would this person/entity be allowed to open the records? Should there be some type of legal action involved? Our study revealed that most approaches tackling this issue do not offer a satisfactory solution. Privacy assurance and management is a complex task and cannot be isolated into independent entities to be handled by one or another of the service participants (*i.e.*, the patient, service provider, medical personnel and the cloud owner). Collaborative approaches to this issue may present some feasible solutions where responsibilities and control are distributed among different participants rather than only one. However, the issue of trust becomes a very delicate point and everyone needs to contribute into building solutions that would increase the participants trust levels in each other and in the system itself.

Beyond security, other challenges and issues arise including the lack of standards and guidelines governing the design, implementation and utilization of e-Health Cloud. This is mostly the responsibility of the cloud owners and the authoritative entities in the Internet and Cloud world. Some level of understanding should be reached that will help in setting up the proper environment where such authorities can collaborate and come up with acceptable guidelines for the e-Health Cloud services. Such guidelines could then be used as the ground work for standardization and better interoperability among different Cloud owners, service providers and users. In addition, the ownership (of data, services, applications, *etc.*) issues, orchestrating services among the different stakeholders, and flexibility and interoperability are also issues that must be addressed. Many of these issues are being addressed and some have been solved. However, more effort is needed and we believe that setting up proper guidelines and development environments will help in this regard. As in the general Cloud services, the e-Health Cloud represents a brilliant approach to support healthcare providers, especially those that cannot afford to build and maintain their own HIT system in-house. Yet, to make this a reality, the research community and the IT industry must put aside their differences and start working together to come up with efficient and workable solutions to the issues and challenges we are currently facing.

7. Conclusions

The e-Health Cloud represents an enabling technology for many healthcare providers to face many challenges such as rising healthcare delivery costs, information sharing, and shortage of healthcare professionals. However, the benefits gained are offset by issues of trust, privacy, and security in addition to several technical issues that must be addressed before healthcare providers can fully adopt and trust the e-Health Cloud.

A literature review of e-Health Cloud issues was presented in this paper with emphasis on the importance of the concepts involved, implementations and challenges. We highlighted the different facets that contribute to building the e-Health Cloud according to four categories: (1) cloud-based storage solutions and HIT applications and systems; (2) platform solutions; (3) e-Health Cloud implementation models; and (4) security solutions for the e-Health Cloud. We described the major technical and non-technical challenges facing the e-Health Cloud which hinder its large scale diffusion. We also discussed several proposed solutions to address the challenges and we concentrated on the security and privacy issues in e-Health Cloud as they represent the biggest challenges.

Despite all the efforts, the e-Health Cloud is still in its infancy. The models so far proposed including the ones we discussed in this paper offer the beginnings of more comprehensive approaches that will satisfy the requirements of the healthcare providers and other relevant entities. Several approaches offer promising solutions, yet they need to clear out the wrinkles and enhance their techniques to be usable. The healthcare industry is huge and in desperate need of effective, highly available, secure and low cost IT solutions. Therefore, it is extremely beneficial for the cloud owners and service providers to invest in the e-Health Cloud and offer comprehensive services that will cater for this sector’s needs and facilitate its operations.

Acknowledgments

The authors of this paper would like to express their gratitude to the anonymous reviewers. Their valuable comments contributed towards the improvement of the paper. The authors would also like to thank Nabeel Al-Qirim for his feedback in some parts of the paper. Additionally we would like to thank Heba AbuKhousa for her help in drawing the figure.

References

1. Goldschmidt, P.G. HIT and MIS: Implications of health information technology and medical information systems. *Commun. ACM* **2005**, *48*, 69–74.
2. Davidson, E.; Heslinga, D. Bridging the IT adoption gap for small physician practices: An action research study on electronic health records. *Inf. Syst. Manag.* **2006**, *24*, 15–28.
3. Klein, R. An empirical examination of patient-physician portal acceptance. *Eur. J. Inf. Syst.* **2007**, *16*, 751–761.
4. Young, H.M. Challenges and solutions for care of frail older adults. *Online J. Issues Nurs.* **2003**, *8*, 5.
5. *HEALTHCAST 2020: Creating a Sustainable Future*. PricewaterhouseCoopers: London, UK, 2006.
6. Singh, H.; Naik, A.D.; Rao, R.; Petersen, L.A. Reducing diagnostic errors through effective communication: Harnessing the power of information technology. *J. Gen. Internal Med.* **2008**, *23*, 489–494.
7. Douglas, T.J.; Ryman, J.A. Understanding competitive advantage in the general hospital industry: Evaluating strategic competencies. *Strateg. Manag. J.* **2003**, *24*, 333–347.
8. Lenz, R.; Reichert, M. IT support for healthcare processes—Premises, challenges, perspectives. *Data Knowl. Eng.* **2006**, *61*, 39–58.
9. Saranummi, N. In the spotlight: Health information systems. *IEEE Rev. Biomed. Eng.* **2008**, *1*, 15–17.
10. Saranummi, N. In the spotlight: Health information systems—PHR and value based healthcare. *IEEE Rev. Biomed. Eng.* **2009**, *2*, 15–17.
11. Saranummi, N. In the spotlight: Health information systems—Mainstreaming mHealth. *IEEE Rev. Biomed. Eng.* **2011**, *4*, 17–19.
12. Vasilakos, A.V.; Lisetti, C. Special section on affective and pervasive computing for healthcare. *IEEE Trans. Inf. Technol. Biomed.* **2010**, *14*, 183–359.
13. Foster, I.; Zhao, Y.; Raicu, L.; Lu, S. Cloud Computing and Grid Computing 360-Degree Compared. In *Proceedings of the Grid Computing Environments Workshop (GCE)*, Austin, TX, USA, 12–16 November 2008; pp. 1–10.
14. Shimrat, O. Cloud Computing and Healthcare. Available online: http://www.himss.org/content/files/Code%2093_Shimrat_CloudComputingandHealthcare_2009.pdf (accessed on 28 June 2012).
15. Teng, C.C.; Mitchell, J.; Walker, C. A Medical Image Archive Solution in the Cloud. In *Proceedings of the 2010 IEEE International Conference on Software Engineering and Service Sciences (ICSESS)*, Beijing, China, 16–18 July 2010; pp. 431–434.
16. Cloud Computing: Clear Benefits: The Emerging Role of Cloud Computing in Healthcare Information Systems. Available online: http://www.techrepublic.com/whitepapers/cloud-computing-clear-benefits-the-emerging-role-of-cloud-computing-in-healthcare-information-systems/2384337 (accessed on 28 June 2012).
17. Kaletsch, A.; Sunyaev, A. Privacy Engineering: Personal Health Records in Cloud Computing Environments. In *Proceedings of the 32nd International Conference on Information Systems (ICIS 2011)*, Shanghai, China, 4–7 December 2011; pp. 1–11.

18. Mahony, M. Trust remains key barrier to eHealth. Available online: http://euobserver.com/893/31958 (accessed on 28 June 2012).
19. Zhang, T.; Liu, L. Security Models and Requirements for Healthcare Application Clouds. In *Proceedings of the IEEE 3rd International Conference on Cloud Computing*, Miami, FL, USA, 5–10 July 2010; pp. 268–275.
20. Maria, A.F.; Fenu, G.; Surcis, S. An Approach to Cloud Computing Network. In *Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance*, Bogota, Colombia, 10–13 November 2009; pp. 409–410.
21. Lohr, H.; Sadeghi, A.; Winandy, M. Securing the E-Health Cloud. In *Proceedings of the 1st ACM International Health Informatics Symposium (IHI 2010)*, Arlington, VA, USA, 11–12 November 2010; pp. 220–229.
22. AbuKhousa, E.; Najati, H.A. UAE-IHC: Steps towards Integrated E-Health Environment in UAE. In *Proceedings of the 4th e-Health and Environment Conference in the Middle East*, Dubai, UAE, 30 January 2012–2 February 2012.
23. Kaletsch, A.; Sunyaev, A. Privacy Engineering: Personal Health Records in Cloud Computing Environments. In *Proceedings of the International Conference on Information Systems (ICIS 2011)*, Shanghai, China, 4–7 December 2011.
24. European Commission. Protecting Your Personal Data. Available online: http://ec.europa.eu/justice/data-protection/individuals/index_en.htm (accessed on 28 June 2012).
25. U.S. Department of Health & Human Services. Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule. Available online: http://privacyruleandresearch.nih.gov/pdf/HIPAA_Booklet_4-14-2003.pdf (accessed on 28 June 2012).
26. ITU-T Technology Watch Report—Standards and eHealth. Available online: http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000120003PDFE.pdf (accessed on 28 June 2012).
27. Wootton, R.; Patil, N.G.; Scott, R.E.; Ho, K. *Telehealth in the Developing World*, Electronic Version; Royal Society of Medicine Press/IDRC: London, UK, 2009.
28. Agency for Healthcare Research and Quality. Available online: http://www.ahrq.gov/ (accessed on 28 June 2012).
29. The US Government Printing Office (GPO). Public Law 111—5—American Recovery and Reinvestment Act of 2009. Available online: http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf (accessed on 28 June 2012).
30. Commonwealth Secretariat. Progress report. Available online: http://www.thecommonwealth.org/files/189921/FileName/HealthProgressReports-E-Health.pdf (accessed on 28 June 2012).
31. Momtahan, L.; Lloyd, S.; Simpson, A. Switched Lightpaths for E-Health Applications: Issues and Challenges. In *Proceedings of the Twentieth IEEE International Symposium Computer-Based Medical Systems (CBMS'07)*, Maribor, Slovenia, 20–22 June 2007; pp. 459–464.
32. Agrawal, D.; Abbadi, A.; Antony, S.; Das, S. Data Management Challenges in Cloud Computing Infrastructures. In *Proceedings of the 6th International Workshop on Databases in Networked Information Systems (DNIS 2010)*, Aizu-Wakamatsu, Japan, 29–31 March 2010.
33. Hasan, J. Effective telemedicine project in Bangladesh: Special focus on diabetes health care delivery in a tertiary care in Bangladesh. *Telemat. Inform.* **2012**, *29*, 211–218.

34. Rayport, J.F.; Heyward, A. Envisioning the Cloud: The Next Computing Paradigm. A MarketspaceNext Point of View. Available online: http://marketspacenext.com/inthemedia/ envisioning-the-cloud/ (accessed on 28 June 2012).
35. *Introduction to Cloud Computing Architecture*. Sun Microsystems: Santa Clara, CA, USA, 2009.
36. Varia, J. Cloud Architectures. Available online: http://aws.amazon.com/articles/ 1632?_encoding=UTF8&jiveRedirect=1 (accessed on 28 June 2012).
37. Hosseini, A.; Sommerville, I.; Sriram, I. Research Challenges for Enterprise Cloud Computing. Available online: http://arxiv.org/abs/1001.3257 (accessed on 28 June 2012).
38. Mei, L.; Chan, W.K.; Tse, T.H. A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues. In *Proceedings of the Asia-Pacific Services Computing Conference (APSCC'08)*, Yilan, Taiwan, 9–12 December 2008; pp. 464–469.
39. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; Zaharia, M. Above the Clouds: A Berkeley View of Cloud Computing. Available online: http://inst.cs.berkeley.edu/~cs10/fa10/lec/20/2010-11-10-CS10-L20-AF-Cloud-Computing.pdf (accessed on 29 June).
40. Sriram, I.; Khajeh-Hosseini, A. Research Agenda in Cloud Technologies. In *Proceedings of the 1st ACM Symposium on Cloud Computing*, *SOCC 2010*, Indianapolis, IN, USA, 10–11 June 2010.
41. Youseff, L.; Butrico, M.; da Silva, D. Toward a Unified Ontology of Cloud Computing. In *Proceedings of the Grid Computing Environments Workshop (GCE'08).* Austin, TX, USA, 12–16 November 2008; pp. 1–10.
42. Leavitt, N. Is cloud computing really ready for prime time? *Computer* **2009**, *42*, 15–20.
43. Vaquero, L.M.; Rodero-Merino, L.; Caceres, J.; Lindner, M. A Break in the clouds: Towards a cloud definition. *ACM SIGCOMM Comput. Commun. Rev.* **2009**, *39*, 50–55.
44. Rimal, B.P.; Jukan, A.; Katsaros, D.; Goeleven, Y. Architectural requirements for cloud computing systems: An enterprise cloud approach. *J. Grid Comput.* **2011**, *9*, 3–26.
45. Al-Jaroodi, J.; Mohamed, N. Service-oriented middleware: A survey. *J. Netw. Comput. Appl.* **2012**, *35*, 211–220.
46. Nguyen, D.K.; Lelli, F.; Papazoglou, M.P.; van den Heuvel, W.-J. Blueprinting Approach in Support of Cloud Computing. *Future Internet* **2012**, *4*, 322–346.
47. Chow, R.; Golle, P.; Jakobsson, M.; Shi, E.; Staddon, J.; Masuoka, R.; Molina, J. Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. In *Proceedings of the 2009 ACM Workshop on Cloud Computing Security,* Chicago, IL, USA, 9–13 November 2009; pp. 85–90.
48. Pearson, S. Taking Account of Privacy when Designing Cloud Computing Services. In *Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing at CLOUD'09*, Washington, DC, USA, 23 May 2009; pp. 44–52.
49. Goldman, J.; Hudson, Z. Virtually exposed: Privacy and e-health. *Health Aff.* **2000**, *19*, 140–148.
50. Kelly, E.P.; Unsal, F. Health information privacy and e-healthcare. *Int. J. Healthc. Technol. Manag.* **2002**, *4*, 41–52.
51. International Classification of Diseases (ICD). Available online: http://www.who.int/ classifications/icd/en/ (accessed on 11 May 2012).

52. Cote, R.A. Architecture of SNOMED: Its Contribution to Medical Language Processing. In *Proceedings of the Annual Symposium on Computer Applied Medical Care*, Washington, DC, USA, 25–26 October 1986; pp. 74–80.
53. Guo, L.; Chen, F.; Chen, L.; Tang, X. The building of cloud computing environment for e-health. In *Proceedings of the International Conference on e-Health Networking, Digital Ecosystems and Tech. (EDT)*, Shenzhen, China, 17–18 April 2010; pp. 89–92.
54. Chen, P.; Freg, C.; Hou, T.; Teng, W.-G. Implementing RAID-3 on Cloud Storage for EMR System. In *Proceedings of the 2010 International Computer Symposium (ICS)*, Taiwan, 16–18 December 2010; pp. 850–853.
55. Rolim, C.O.; Koch, F.L.; Westphall, C.B. A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions. In *Proceedings of the Second International Conference on eHealth, Telemedicine, and Social Medicine (ETELEMED'10)*, St. Maarten, The Netherlands, 10–16 February 2010; pp. 95–99.
56. Lo, O.; Fan, L.; Buchanan, W.; Thümmler, C.; Khedim, A.; Lawson, A.; Uthmani, O.; Bell, D. Patient Simulator: Towards Testing and Validation of e-Health Infrastructures. In *Proceedings of the Pervasive Health*, Dublin, Ireland, 23–26 May 2011.
57. White, J. Cloud Computing in Healthcare: Is there a Silver Lining? Available online: http://www.aspenadvisors.net/results/whitepaper/cloud-computing-healthcare-there-silver-lining (accessed on 28 June 2012).
58. Fan, L.; Buchanan, W.; Thummler, C.; Lo, O.; Khedim, A.; Uthmani, O.; Lawson, A.; Bell, D. DACAR Platform for eHealth Services Cloud. In *Proceedings of the 4th International Conference on Cloud Computing*, Miami, FL, USA, July 2011; pp. 219–226.
59. Baru, C.; Botts, N.; Horan, T.; Patrick, K.; Fedman, S.S. A Seeded Cloud Approach to Health Cyberinfrastructure: Preliminary Architecture Design and Case Applications. In *Proceedings of the 45th Hawaii International Conference on System Sciences*, Maui, HI, USA, 4–7 January 2012; pp. 2727–2734.
60. He, C.; Jin, X.; Zhao, Z.; Xiang, T. A Cloud Computing Solution for Hospital Information System. In *Proceedings of the Intelligent Computing and Intelligent Systems (ICIS)*, Xiamen, China, 29–31 October 2010; pp. 517–520.
61. Yu, W.D. A Service Modeling Approach to Service Requirements in SOA and Cloud Computing—Using a U-Healthcare System Case. In *Proceedings of the IEEE 13th International Conference on e-Health Networking, Applications and Services*, Columbia, MO, USA, 13–15 June 2011; pp. 233–236.
62. Rosado, D.G.; Gómez, R.; Mellado, D.; Fernández-Medina, E. Security analysis in the migration to cloud environments. *Future Internet* **2012**, *4*, 469–487.
63. Grobauer, B.; Walloschek, T.; Stocker, E. Understanding cloud computing vulnerabilities. *IEEE Secur. Privacy Mag.* **2011**, *9*, 50–57.
64. Li, M.; Yu, S.; Ren, K.; Lou, W. Securing Personal Health Records in Cloud Computing: Patient-centric and Fine-grained Data Access Control in Multi-owner Settings. In *Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010)*, Singapore, 7–9 September 2010; pp. 89–106.

65. Yu, S.; Wang, C.; Ren, K.; Lou, W. Achieving secure, scalable and fine-grained data access control in cloud computing. In *Proceedings of INFOCOM 2010*, San Diego, CA, USA, 15–19 March 2010; pp. 1–9.
66. Ahmed, S.; Raja, M.Y.A. Tackling cloud security issues and forensics model. In *Proceedings of the High-Capacity Optical Networks and Enabling Technologies (HONET 2010)*, Cairo, Egypt, 19–21 December 2010; pp. 190–195.