International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 1 (2018) pp. 456-470


# Survey on eHealth Cloud Security Challenges

**[1]Yazan Al-Issa, [2]Mohammad Ashraf Ottom and [1]Ahmed Tamrawi**

*[1]Computer Engineering Department, Yarmouk University, Irbid 21163, Jordan.*
*[2] Computer Information Systems Department, Yarmouk University, Irbid 21163, Jordan*

*ORCID {0000-0001-7747-1183, 0000-0002-6751-8811, 0000-0003-4833-1995}*

**Abstract**

Cloud computing is a promising technology that is expected to transform the healthcare industry. Cloud computing has many benefits like flexibility, cost and energy savings, resource sharing, and fast deployment. In this paper, we study the use of cloud computing in the healthcare industry and different cloud security challenges. The centralization of data on the cloud moves data ownership to the cloud service provider. A lot of healthcare providers are reluctant to accept this loss of control over their sensitive data. As a result, security, efficiency, and scalability concerns are hindering the wide adoption of the cloud technology. In this work, we found that state of the art solutions addresses only a subset of those concerns. Thus, there is an immediate need for a holistic solution that balances all the contradicting requirements.

**Keywords:** eHealth, cloud computing, healthcare, security.

## INTRODUCTION

Cloud computing is a relatively new technology that will have a great impact on our lives. Using this technology, it is possible to access computing resources and facilities anytime and anywhere. Healthcare industry is continuously evolving, and the future healthcare model is anticipated to be information centric. The industry can benefit from the cloud technology to manage change and complexity. This promising technology can help facilitate communication, collaboration, and coordination among different healthcare providers. The cloud can help the healthcare industry deliver more value for the dollar. It can offer fast, flexible, scalable, and cost-effective infrastructure and applications. The cloud can help store, manage, protect, share, and archive Electronic Health Records (EHRs), laboratory information system, pharmacy information system, and medical images. Overall, patients will obtain better care because of up-to-date health records and continuous interactions between different healthcare providers. Beside the lack of standards, regulations, and interoperability problems, the main obstacles that are hindering the wide-scale adoption of the cloud by healthcare providers are the security, confidentiality, and trust issues [1].

Cloud computing offers opportunities and challenges. Just like every other IT application, the cloud has various security issues and concerns. Since it usually operates in an open and shared environment, it is vulnerable for data loss, theft and malicious attacks. Weak cloud security is one of the important problems that is hindering the full diffusion of the cloud in healthcare industry. Healthcare professionals have many reasons not to trust the cloud, for example, they cannot give away control over their medical records. Cloud providers usually store their data in different data centers located in different geographic locations. This represents a clear advantage, since data storage on the cloud will be redundant, and in case of force majeure, different data centers will help recover from disasters. On the other hand, this same advantage can pose a security challenge, because data stored in different locations will be more prone to theft and loss. In general, there are many security risks associated with the use of the cloud like: failure to separate virtual users, identity theft, privilege abuse, and poor encryption are among the security concerns [2].

The goal of this paper is to survey literature [3], [4], review the state of the art to understand various cloud security challenges and available solutions. This paper tries to answer the following research questions:

**RQ1.** What are the cloud computing schemes used in healthcare systems?

**RQ2.** What are the security challenges hindering the wide-scale adoption of cloud computing by healthcare providers?

**RQ3.** What are the state of the art cloud computing solutions used by current healthcare providers and the security risks associated with those solutions?

The remainder of the paper is organized as follows; Section II presents background information about cloud computing. Section III discusses the security requirements needed by healthcare providers for adopting cloud computing. In Section IV, we survey recent work addressing security risks for eHealth systems using cloud computing. Available security solutions are discussed in Section V. A case study comparing two online web-based services particularly Google Health and Microsoft HealthVault is presented in Section VI. Finally, our findings and conclusions are summarized in Section VII.

## CLOUD COMPUTING

### *A. Cloud Definition*

There are multiple cloud definitions, different people, different research groups, and different papers tend to define the cloud in different ways. Nowadays, cloud computing is more of a buzzword rather than a scientific term. According to the National Institute of Standards and Technology (NIST) special publication [5] "*cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that*

*can be rapidly provisioned and released with minimal management effort or service provider interaction*". Anyone who delivers technology over the internet seems to think that he is using the cloud technology. Only few papers that uses the cloud term exactly meets the NIST models and characteristics.

### *B. Cloud Computing Characteristics*

According to the official definition, cloud computing has five main characteristics: resource pooling, broad network access, rapid elasticity, on-demand self-service, and measured service [5].

- *Shared Resources*: clients can share resources like networks, servers, storage, software, memory and processing simultaneously. Providers can dynamically allocate resources according to the fluctuations in demand, and the client is completely unaware of the physical locations of these services.
- *Broad network access*: the cloud allows a broad access to the network using the internet from any device.
- *Elasticity*: the cloud is flexible and configurable. Clients feel that resources are unlimited.
- *On-demand self-service*: if needed, any customer can automatically configure the cloud without the interference of service technicians. Customers perform scheduling and decides the required storage and computing power.
- *Measured service*: different cloud services can be measured using different metrics. Detailed usage reports are generated to preserve the rights of customers and providers.

### *C. Service Models*

Cloud computing has four different service models [5]–[8]:

- *Software as a Service (SaaS)*: most popular cloud service, the software resides on the provider platform, the consumer access the software using a web browser or an Application Programming Interface (API). It follows a pay-per-use business model. Consumers do not need to worry about software upgrades and maintenance, some limited application configuration capability might be available to consumers. Salesforce [9] and Office 365 [10] are popular examples.
- *Platform as a Service (PaaS)*: provides development and testing environments. The consumer develops his own application on a virtual server, and has some control over the application hosting environment particularly the application and data. Making it faster to develop, test, and deploy applications. Cloudfoundry [11] is a good example.
- *Infrastructure as a Service (IaaS)*: provides the infrastructure, operating systems, and applications. It is the service of choice for companies that do not have the necessary capital to buy hardware. Customers pay according to consumption. Infrastructure is scalable depending on processing and storage needs. The consumer has control over applications, data, middleware, and operating systems, but not over the underlying cloud infrastructure. Amazon EC2 [12] is a good example.
- *Anything as a Service (XaaS)*: offers a variety of services ranging from personal services to large resources over the internet [13], [14].

### *D. Delivery Models*

Cloud computing has five different delivery models [5], [6], [8]:

- *Private Cloud*: located on premises, over the intranet, behind the firewall, and usually managed by the same organization that uses it. Their services are offered to the organization employees. Security issues are limited; a good example is VMware [15].
- *Public Cloud*: located off premises, over the internet, and usually managed by a cloud service provider. Their services are offered to the public. It is less secure than the private cloud, some popular public clouds are Dropbox [16], Amazon EC2 [12], and Microsoft Azure [17].
- *Hybrid Cloud*: combines private and public clouds, and it has trust and confidentiality issues because of the public part. A good example is Rackspace [18].
- *Community Cloud*: a group of entities with a common goal share the cloud, universities usually share a single cloud. A good example is NYSE Capital Markets Community Platform [19].

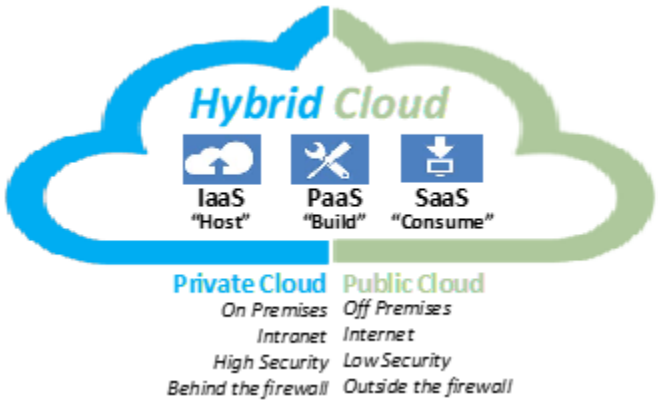


**Figure 1.** Relationship between Delivery and Service Models.

### *E. eHealth Cloud Benefits*

The cloud has many benefits [20], [21]:

- Improved patient care because of the continuous interaction by the patient with different healthcare stakeholders. Patient data is available anytime, and anywhere for doctors to analyze and diagnose.

- Cost savings: there is no need to buy expensive hardware and software. Savings include the direct cost of purchasing on-premise hardware and software also the support and maintenance costs.
- Energy savings: the energy bill will be cut because there is no need for data centers on premises, as a result there is no need for expensive cooling.
- Robust disaster recovery: in case of emergency almost all cloud service providers offer a redundant system and services.
- Research: the cloud is a central data repository that can be used to support national medical research, disease control, and epidemics monitoring.
- Solving the scarcity of resources: Doctors in remote areas can use telemedicine to perform consultations.
- Rapid deployment: Software and hardware systems can be used almost immediately.
- Data availability: data is available for all healthcare stakeholders like physicians, clinics, hospitals, and insurance companies.

### *F. eHealth Cloud Limitations*

The cloud has many limitations [6], [7], [20], [21]:

- *Availability and reliability*: the service can be slow, interrupted or down depending on the strength of the internet connection. This will largely affect user experiences.
- *Interoperability*: there is a need for standards to achieve proper communication, coordination and collaboration between different healthcare providers platforms.
- *Security and privacy*: open and shared environment is prone to data loss and theft.
- *Legislation & Regulations*: the wide adoption of cloud computing requires laws, regulations, and ethical and legal frameworks.
- *Limited control and flexibility*: limited control over data ownership because of centralization. The cloud applications are often generic, and custom software might be hard to rent.
- *Vulnerability to attacks*: the cloud is prone to different kind of security attacks.

## COMMON eHealth SECURITY ISSUES

Nowadays, healthcare is centered on accessing medical records anytime and anywhere. The use of cloud computing paradigm in healthcare facilitates medical records sharing and integration. Even though, the cloud computing paradigm offers several benefits, it also poses privacy and security threats to the health data [21]. Essentially, the cloud service providers should deal with security concerns in the cloud to enhance the trust level between the patients and healthcare providers [22]–[24]. In this section, we discuss important security requirements for eHealth systems to address the arising security and privacy issues hindering the wide-scale adoption of cloud computing by healthcare providers.

There is a long line of research pertaining to the security requirements of healthcare cloud applications. For example, the ISO/TS 18308 standard [25] defines the security and privacy issues for EHRs. The International Medical Informatics Association (IMIA) investigated the issues of data protection and security in healthcare networked systems [26]. US Health and Human Services (HHS) published a report [26] about Personal Health Records (PHRs), aiming at developing PHRs and PHR systems to put forward a vision that "*would create a PHR that patients, doctors and other healthcare providers could securely access through the Internet no matter where a patient is seeking medical care.*" In [27], Bakker *et al.* present a brief overview on cloud computing security in terms of security considerations, models, threats and precautions. Avancha *et al.* [28] examine the privacy requirements of mobile computing technologies that have the potential to transform healthcare industry. Through an extensive survey of literature, Avancha *et al.* propose a conceptual privacy framework for healthcare applications. In [29], Ardagna *et al.* present an extensive survey on the interface between cloud security and cloud security assurance. They first provide an overview of the state of the art on cloud security. Then, they introduce the notion of cloud security assurance and analyze its growing impact on cloud security approaches. Finally, they present some recommendations for the development of next-generation cloud security and assurance solutions. Ibrahim *et al.* [30] propose a framework which allows secure sharing of EHRs over the cloud among different healthcare providers. The framework ensures the confidentiality, integrity, authenticity, availability and auditability of EHRs. Along the line, Abbas *et al.* [24] present an extensive survey that aims to encompass the state of the art privacy-preserving approaches employed in eHealth clouds. They also classify the privacy-preserving approaches into cryptographic and non-cryptographic approaches. Furthermore, the strengths and weaknesses of the presented approaches are reported and some open issues are highlighted. [31] reports on the results of a systematic literature review concerning the security and privacy of EHR systems.

The eHealth system security and privacy concerns do not only deal with abiding by the Confidentiality, Integrity and Availability (CIA) security model [32]. In [33], Metri *et al.* argue that security threats to the cloud data include spoofing identity via an attacker pretending to be a valid user, tampering with the data that involves malicious alterations and modification of the content, repudiation with the users who deny their signature authenticity after performing an activity with the data, and information disclosure via the exposure of information to unauthorized users [33]. For example, the use and disclosure of the Protected Health Information in the USA should be in accordance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA). The Act considers the confidentiality of health data to be an obligation, not an option [34]. To improve the trust in this relatively new technology,

cloud computing applications have multiple security requirements to be fulfilled. Below, we outline the important security and privacy requirements for healthcare application clouds.

### *A. Confidentiality*

Confidentiality is the act of ensuring that patients health data is kept completely undisclosed to unauthorized entities. Delegating data control to the cloud, leads to an increase in the risk of data compromises, as the data becomes accessible to an augmented number of parties. Due to the increased number of parties, devices and applications involved, there is an increase in data compromise threats. To make the patient/doctor relationship work effectively, it is necessary for the patient to trust the healthcare system to protect the confidentiality of his data. If the patient feels that the information he gives to his doctor is not protected, and that his privacy is threatened, he can be more selective about the information he will provide to his doctor in the future. The threat of data compromise can harm the patient/doctor relationship and hamper the proper medical diagnosis and treatment [35]. For example, an employer may refuse a job if the patient's medical data are disclosed. Confidentiality can be achieved by access control and using encryption techniques.

### *B. Integrity*

Integrity ensures the health data captured by a system or provided to any entity is accurate and consistent with the intended information and has not been modified in any way [36]. Using the cloud for an important application like eHealth cloud requires assurances of good reliability for the provided services. All eHealth cloud services and data must be error-free. Improper treatment based on erroneous data can have serious consequences on patients' health. The HIPAA Security Rule (*Section 164.312(c)(1) Integrity*) [37] states that covered entities must "*implement policies and procedures to protect electronic personal healthcare information from improper alteration or destruction.*" In a healthcare setting, services that stores and manipulates patient data must implement integrity and verification functionality, like non-medical applications, via the means of a checksum or a hash, before using the data. If the integrity check fails, the healthcare application must report an error and terminate without processing the data. For example, Blough *et al.* [38] have proposed the use of 21 trees to store public healthcare records.

### *C. Availability*

For any healthcare cloud system to serve its purpose, the information must be available all the time. An important and often overlooked aspect in the eHealth system is the availability of data in critical situations including the ability to carry on operations even when some authorities misbehave and the ability to continue operations even in the possibility of a security breach. High availability systems should prevent service disruptions due to power outages, hardware failures, system upgrade, and denial-of-service attacks. It should also be able to preserve the usability of healthcare records after enforcing HIPAA security and privacy rules.

### *D. Ownership & Privacy of Healthcare Information*

In general, the owner is defined as the creator of the information. Establishing information ownership is necessary for protection against unauthorized access or misuse of patient's medical information. Ownership of healthcare information can be protected through a combination of encryption and watermarking techniques that results in secured healthcare information that cannot be transmitted, accessed, or released without the mutual acceptance of all entities involved in the ownership/creation of the healthcare information. Patients can allow or deny the sharing of their information with other healthcare practitioners [33]. To implement patient data sharing in a healthcare system, patient may grant rights to users based on a role or attributes held by the respective user to share specific healthcare data with that user.

### *E. Authenticity*

Authenticity in general refers to the truthfulness of origins, attributions, commitments, and intentions. It ensures that the entity requesting access is authentic. In healthcare systems, the information provided by the healthcare providers and the identities of the entities using such information must be verified via the Authentication Act [39]. The authentication of information can pose special problems, like man-in-the-middle attacks, and is often mitigated with a combination of usernames and passwords. Most cryptographic protocols include some form of endpoint authentication specifically to prevent man-in-the-middle attacks. In a healthcare system, both healthcare information offered by providers and identities of consumers should be verified at every access.

### *F. Non-repudiation*

Repudiation threats are concerned with the users who deny their signature authenticity after accessing health data [40]. For instance, in the healthcare scenario neither the patients nor the doctors can deny their signature authenticity after misappropriating the health data. Just like electronic commerce, healthcare cloud applications can leverage digital signatures and encryption to establish authenticity and non-repudiation.

### *G. Audit*

Auditing is a security measure that ensures the safety of a healthcare system. Audit means recording user activities of the healthcare system in chronological order, such as maintaining a log of every access and modification of data. Both HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) require users within the healthcare provider's organization to be held accountable for their actions when handling patients' protected health information. There are different approaches to maintaining

audit controls for such information; for example, Integrating the Healthcare Enterprise (IHE) [41] specifies a profile for the Audit Trail that contains sufficient information to answer questions such as: "*For some user: which patient's records was accessed? For some patient's record: which users accessed it? What user authentication failures were reported?*" Such approaches could help administrators mitigate insider threats by ensuring detection of unauthorized access and illegal disclosure of healthcare records. Auditing could also help detect attempts by hackers to break into a public healthcare cloud system and help administrators detect potential vulnerabilities in the system.

### *H. Access Control*

Access control is a mechanism for controlling access to a patient's public health information that restricts access to legitimate entities only. The access control policy is typically based on the privilege and right of each authorized practitioner by patient or a trusted third party. Several solutions have been proposed to address the security and access control concerns. Role-Based Access Control (RBAC) [42], [43] and Attribute-Based Access Control (ABAC) [44], [45] are the most popular models for healthcare application clouds.

### *I. Data Remanence & Freshness*

Data remanence refers to the residual representation of data that have been in some way nominally erased or removed. Data remanence may cause an unintentional data confidentiality attack. In healthcare system, data confidentiality and integrity are not enough if data freshness is not considered. Data freshness implies that the patient health records must be fresh and up-to-date. Delays in storage and sending outdated notifications results in data inconsistency especially in critical situations.

### *J. Anonymity*

Anonymity refers to the state where a patient cannot be identified from his public health records acquired for research and quality improvement. For instance, identities of the patients can be made anonymous when they store their health data on the cloud so that the cloud servers could not learn about the identity. The HIPAA Privacy Rule states that covered entities may use or disclose public healthcare information that is de-identified without restriction [46], [47]. Covered entities that seek to release such data must determine that the information has been de-identified using either statistical methods to verify de-identification or by removing certain parts of the data. Under the HIPAA Privacy Rule, a covered entity can de-identify public healthcare record by removing all 18 elements that could be used to identify the patient or the patient's relatives, employers, or household members. The rule also requires the covered entity to have no actual knowledge that the remaining information could be used alone or in combination with other information to identify the patient. Some of the 18 identifiable elements are the patient's name, geographical information such as ZIP code, phone number, all elements of dates except the year, and biometrics. Anonymization in healthcare data setting is an active area of research, with extensive literature; Appari *et al.* [48] provide a useful overview by citing several research efforts aimed at anonymizing patient data: global and local recoding [49], confidential audits of medical record access [50], micro-aggregation [51] and data perturbation [52].

### *K. Unlinkability*

Unlinkability refers to the use of resources or items of interest multiple times by a user without other users or subjects being able to interlink the usage of these resources [53]. This means that the probability of those items being related from the attacker's perspective stays the same before and after the attacker's observation.

### *L. Cloud Multi-Tenancy*

Clouds were built for several reasons of which one of the most important reasons were: shared computing, shared memory, and shared storage. Cloud providers deploy multi-tenancy as a standard to achieve efficient utilization of resources, while decreasing cost. Thus, security threats prevail to data access and management to secure data sharing and integration. To deliver secure multi-tenancy, there should be isolation among patients data [54], [55].

### *M. Secure Transmission*

The HIPAA Security Rule (*Section 164.312(e) Transmission Security*) states that covered entities must "*implement technical security measures to guard against unauthorized access to electronic protected health information … transmitted over an electronic communications network*" [37]. The 2009 HITECH Act extends this rule to business associates [46], [47]. Although HIPAA's rule covers communication between HIPAA-covered entities, the concern here is an adversary who wishes to obtain confidential medical information from observing the network communications between two communicating nodes. For example, the adversary may inspect the network packets and obtain sensitive medical data; this problem can be solved by encrypting all communications. For example, most emerging services use Hyper Text Transfer Protocol (HTTP) over Secure Sockets Layer (SSL). Even if the network traffic is encrypted, in some settings it is possible for a clever adversary to use traffic analysis via the study of the size and timing of network packets to determine characteristics of the traffic[56]. This is called *side-channel* attacks. Many solutions require the addition of delays (to defeat timing analysis) or padding (to defeat packet-size analysis) [57], [58]. Consequently, these adhoc solutions poses non-negligible overhead on system performance and resource usage.

**RECENT WORK IN eHealth**

There is a vast amount of work that has been done with regard to addressing security and privacy risks in eHealth. In this section, we survey recent work and proposed secure eHealth system architecture.

In [59], Hamid *et al.* target the confidentiality of healthcare patient's multimedia data in the cloud by proposing a tri-party one-round authenticated key agreement protocol based on bilinear pairing cryptography [60]. The proposed protocol can generate a session key among the participants to communicate securely. Finally, the private healthcare data is accessed and stored securely by implementing a decoy technique [61], [62] with a fog computing facility [63], [64]. Nonetheless, the proposed approach incurs a computational overhead cost in communication in sacrifice for strong security.

In [65], Marwan *et al.* propose a novel method based on Shamir's Secret Share Scheme (SSS) [66] and multi-cloud concept to enhance the reliability of cloud storage in order to meet security requirements to avoid loss of data, unauthorized access, and privacy disclosure. The proposed technique divides the secret data into many small shares so that one does not reveal any information about medical records. Besides, mutli-cloud architecture, data are spread across different cloud storage systems. In such a scenario, cloud consumers encrypt their data using SSS technique to ensure confidentiality and privacy. Therefore, the healthcare data are split into various shares so that data confidentiality is guaranteed. On contrary, the paper does not discuss any aspects of the optimal number of shares for the incurred trade-off between efficiency and security. It does not discuss the quality analysis of recovered healthcare data.

In [67], Galletta *et al.* present a system developed at Instituto di Ricovero e Cura a Carattere Scientifico (IRCCS) that is claimed to address the patient's data security and privacy. The presented system is based on two software components the anonymizer and splitter. The first collects anonymize clinical data, whereas the second obfuscates and stores data in multiple cloud storage providers. Thus, only authorized clinical operators can access data over the Cloud. They present a case study that uses Magnetic Resonance Imaging (MRI) data to assess the performance of the implemented system. Alexander *et al.* [68] propose a privacy-aware system and anonymization techniques for data publishing on cloud for PHRs. The proposed system uses k-anonymity [69], [70] and Advanced Encryption Standard (AES).

Smithamol *et al.* [71] address the data confidentiality and access privacy by proposing a novel architecture for the outsourced health records. The proposed model uses partially ordered set for constructing the group based access structure and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [72] to provide fine-grained medical records access control. The proposed approach minimizes the computational overhead and the overall encryption time. Nevertheless, the performance analysis shows the efficiency of the proposed model, making it suitable for practical use. In [73], Sneha *et al.* propose to use *k*-anonymity [69], [70] for privacy-preserving on eHealth records.

Ibrahim *et al.* [74] provide a comprehensive solution to secure access to privacy sensitive EHR data through: (1) a cryptographic role based technique to distribute session keys using Kerberos protocol, (2) location and biometrics based authentication method to authorize the users and (3) a wavelet based steganographic technique to embed EHR data securely in a trusted cloud storage. The paper also shows the resilience of the proposed solution to man-in-the-middle and replay attacks. However, they did not analyze the scalability of the approach and its resilience to other significant security risks including integrity and availability of the data as well as the computational overhead.

The paper [75] lists various methods of encryption and also addresses security and privacy challenges in healthcare cloud by deploying a novel framework with Cloud-based Privacy-aware Role Based Access Control (CPRBAC) model. The side goal is to reduce computational complexity and communication overhead. However, there is no qualitative analysis discussion on the efficiency of the approach and its mitigation to security and privacy attacks.

In [76], Padaki *et al.* survey several healthcare security lapses pertaining to non-repudiation, CIA model, and what it means to stakeholders in the healthcare industry. They also discuss few proven operational strategies, risk management methodologies and discern what the industry can do to mitigate such security risks and privacy threats. The paper classifies the security threats posed on healthcare clouds into three high level categories including: network, system care and protection, and compliance with standard acts and rules.

The paper [77] discusses important concepts related to EHRs sharing and integration in healthcare clouds and analyze the arising security and privacy issues in access and management of EHRs. The paper presents several basic security and privacy requirements for application clouds: ownership, authenticity, non-repudiation, patient consent and authorization, integrity and confidentiality and availability, archiving and auditing. Then they present an EHR security reference model for managing security issues in healthcare clouds, which highlights three important core components in securing an EHR cloud: secure collection and integration, secure storage and access management, and secure usage model. Finally, they illustrate the development of the proposed EHR security reference model through a use-case scenario and describe the corresponding security countermeasures and possible security techniques.

Ibrahim *et al.* [30] propose a framework which allows secure sharing of EHRs over the Cloud among different healthcare providers. In the proposed framework, Public Key Infrastructure (PKI) is used to maintain authentication between participating healthcare providers and the EHR sharing cloud. The proposed framework claims that it ensures the confidentiality, integrity, authenticity, availability and auditability. It also claims that it meets the security standards defined in the technical safeguards of the HIPAA Security Rule.

In [78], the authors present a security architecture for establishing privacy domains in eHealth infrastructures. This architecture is based on Trusted Virtual Domains (TVDs) [79]

that extends the protection of privacy-sensitive data from centrally managed secure networks to the client platforms of the end-users. However, there are still open research challenges not addressed by the presented architecture including: anonymity, non-repudiation, and inability of the patient to authenticate.

## AVAILABLE eHealth SOLUTIONS

Security and privacy issues are among the most talked about topics in information technology and communications fields. Many healthcare providers use cloud technology with caution due to the risks involved such as unauthorized use or access to private and sensitive health data. To mitigate security and privacy concerns, some guidelines and recommendations must be addressed by cloud service providers. All solutions suggested in literature are not holistic in nature, they partially address some of the cloud security problems discussed in Section 3. In the following subsections, we discuss the available solutions from regulatory and technical aspects.

### *A. Regulatory Aspects*

Standards are usually created to describe accepted characteristics of a product or service by experts from organizations and scientific institutions. These standards are documented and published to represent a consensus on characteristics such as quality, security and reliability that should remain applicable for an extended period of time. The standards goal is to support individuals and companies when procuring goods and services. Cloud service providers can boost their reputation by complying with standards. Different countries developed multiple standards to guarantee cloud privacy and security. Below we review US (e.g., HIPAA and HITECH) and international standards (e.g., ISO/IEC 27000 and General Data Protection Regulation (GDPR)).

#### *1) US Standards*

##### *a)* ***HIPAA***

HIPAA is a legal framework for securing healthcare systems. HIPAA required the Secretary of the HHS to set rules, guidelines and acts to protect the privacy and security of health data. As a result, HHS issued HIPAA Security Rule and HIPAA Privacy Rule. The main goal of the Security Rule is to protect the individuals health data in balance with permitting technology bodies to adopt information technology advancement to benefit healthcare services and produce quality services for individuals and healthcare providers. Specifically, The Security Rule requires technology bodies to use administrative, technical, and physical safeguards to protect health data by ensuring the confidentiality, integrity, and availability health data, protect health data against all threats to the security or integrity of data, provide protection against unauthorized use of health data, and ensure technology bodies and services providers compliance [80]. The HIPAA Privacy Rule aims to set standards and guidelines to protect patients medical records. The rule implements appropriate safeguards to protect the privacy of PHR, provide limitation on data uses without patient authorization, grant patients the rights to examine and obtain a copy of their medical records, and allow patients to amend incorrect information [81].

"*Other approaches used to enhance the security level and confidentiality are* [82]*: First, individual identification is deleted during data collection (anonymous data). Secondly, individual identification is initially recorded during data collection and eventually removed. In this type of identification, there is a chance to re-identify the patient because patient information has been recorded at some stage (anonymized data). However, the removal of personal health data requires the removal of data elements like: medical record numbers, social security numbers, Internet Protocol (IP) addresses, health plan beneficiary numbers, email addresses, web Universal Resource Locators (URLs), fax numbers, account numbers, and device identifiers. Removing these data to meet De-identification Act* [83] *can affect the outcome of data analysis* [84]*. Thirdly, encoding and encrypting data, however, there is a chance to reveal the encryption key using advanced computer technology. Privacy advocates and data regulators are gradually complaining about data collection and data usage in Big Data era, and they call for a sophisticated protocol that balance between individual privacy and research benefits*" [85], [86].

##### *b)* ***HITECH***

The HITECH Act is a healthcare legislation created by the HHS meant to widen and accelerate the adoption of EHR and to improve the performance of healthcare systems. The HITECH Act motivates and rewards healthcare providers by offering incentives and grant programs, and increases public trust in EHR by setting appropriate privacy and security measures. It also encourages investments in developing healthcare systems. HITECH Act regulations were motivated by the lack of financial resources, shortage in technical expertise, and the lack of a secure infrastructure for exchanging healthcare information [87]. For example, to overcome the financial obstacles, healthcare providers may obtain up to $63,750 in extra payments if they become an effective user of EHR between 2011 and 2021. In addition, US government has reserved about $650 million under the HITECH Act to create a national infrastructure for health information exchange called the Nationwide Health Information Network and they will establish a set of standards and policies that will ensure secure exchange of health information on the web [87], [88].

#### *2) International Standards*

##### *a)* ***ISO/IEC 27000-series***

The ISO/IEC 27000 series [89] is a series of standards reserved for addressing information security concerns. The series is jointly published by the International Organization for Standardization (ISO) [90] and the International Electrotechnical Commission (IEC) [91]. The ISO/IEC 27000-series brings best practices on information security management within an Information Security Management System (ISMS).

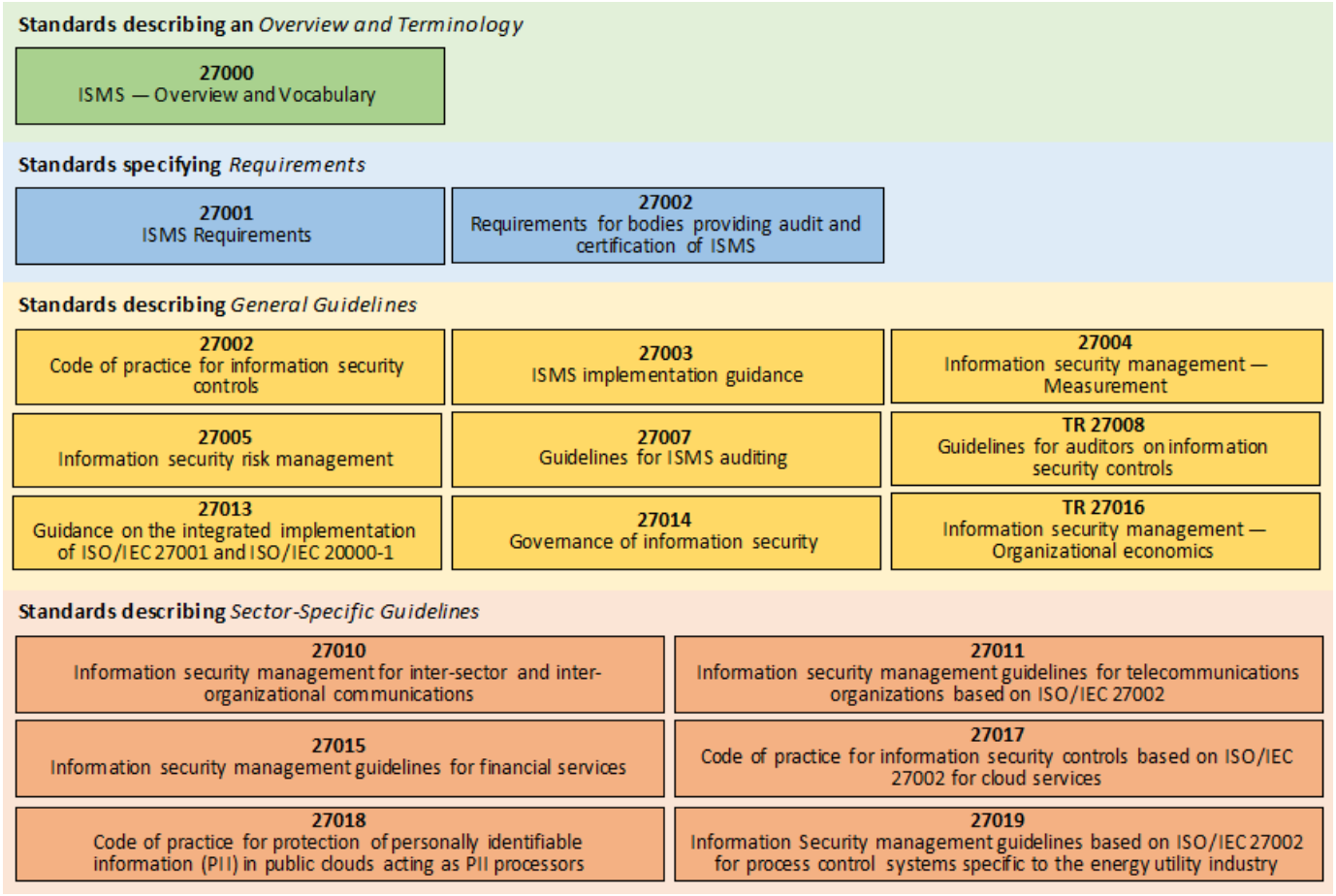


**Figure 2.** ISO/IEC 27000-series standards categories

Figure 2 shows the relationship between different ISO/IEC 27000-series standards. It shows that the ISO/IEC 27000-series standards can be grouped into 4 different categories based on the purpose and scope of each standard. The categories are: (1) *vocabulary and terminology* category that describes the fundamentals of ISMS and defines related terms, (2) *requirement standards* category consists of the standards that provide requirements and guidelines for the development and operation of an ISMS, (3) *guideline standards* category provides a practical implementation guidance for securing information from different angles, (4) *sector-specific guideline standards* category consists of standards that appeal to different industry sectors such as: telecommunication, finance, etc. Below, we present the details of ISO/IEC 27001 and ISO/IEC 27002. The other standards in the ISO/IEC 27000-series are used to guide and support the ISO/IEC 27001/27002 auditing and certification process.

The ISO/IEC 27001 [92] specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized ISMS and their alignment with the organization's strategic goals. ISO/IEC 27001 certification secures information assets and restores patients trust in cloud service providers. The standard adopts the Plan-Do-Check-Act (PDCA) model to structure all ISMS processes. The model ensures that ISMS is established, implemented, assessed, measured where applicable, and continually improved. Currently, the standard defines 114 controls grouped into 14 control objectives. Control objectives include: communications security, cryptography, and information security incident management. Overall, accredited registrars are reporting an increase demand on ISO/IEC 27001 certification from service providers.

The ISO/IEC 27002 [93] standard concentrates on security during system planning and development stages. The standard is structured logically around groups of related security controls. Figure 3 summarizes 19 best practices [94]. For example, section 10 in Figure 3 states "*there should be a policy on the use of encryption, plus cryptographic authentication and integrity controls such as digital signatures and message authentication codes, and cryptographic key management*" [94]. Section 13 in Figure 3 includes controls on network security management and information transfer. It should be noted that ISO/IEC 27002 is a code of practice to adhere to, not a formal certification as ISO/IEC 27001 [95].

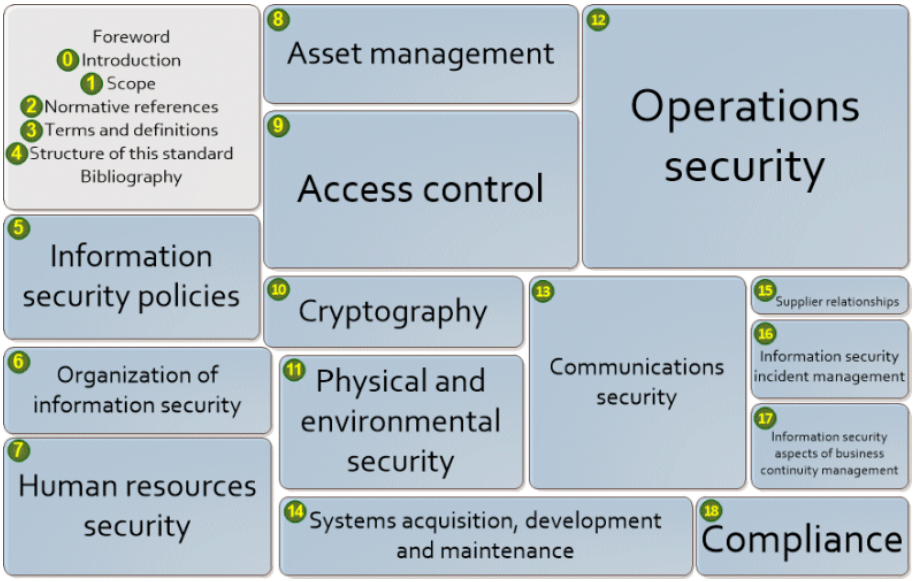


**Figure 3.** ISO-27002 best practice topics [94].

*b) **EU General Data Protection Regulation (GDPR)***

GDPR is the European Union (EU) primary tool that regulates the protection of EU citizens individual data. The recent rule enhances the privacy rights of individuals, and gives authorities a greater power to act against non-compliant organizations. The new rule protects personal data of 500 million EU citizens in all 28 EU member states. They are meant to harmonize local data privacy laws across Europe. The new rules are going to help fight terrorism, it is also going to gain people trust in various digital services, giving a strong boost to the economy [96], [97].

GDPR replaces the old data protection regulation. It is going to be effective starting 25 May 2018, it gives consumers more control over their data, it protects the free movement of personal data within the European Union, it also regulates the export of personal data outside the EU. This act is applicable worldwide, it applies on every organization that is handling EU citizens data. It applies on EU organizations like data controllers, and data processors that collects or process the personal data of EU residents, it also applies on data controllers, data processors that reside outside the EU if they offer goods and services to data subjects that reside in the EU [96], [98], [99].

Cloud service providers should demonstrate compliance by maintaining a log of all data processing activities. They should apply the appropriate personal and organizational measures. Unlike the old Data Protection Directive, noncompliant organizations will face severe punishment for data breaches, the most serious infringement can cost a company twenty million Euros or up to 4% of the annual worldwide turnover whichever is greater [96]. The law opens the door for compensation claims for suffered damages including reputational damages [99]. Under the new regulations, companies should ask for explicit consent from consumers, customers also have the right to opt out, businesses should keep a log of all consumer consents [100]. Privacy by design means that service providers should design their processes to accommodate consumer privacy, they should comply with protection laws, should monitor what personal data they hold, where it came from, whom they share it with, and where do they store a customer data. In addition, data must be used for the reason it was collected [96], [98], [101], [102].

The rights of data subjects are expanded in the new regulation. The new regulation gives consumers the right to be forgotten, data must be permanently erased if requested. Breach notification is mandatory in all member states, the new act expects a company to report data breaches to the regulator and customer within 72 hours or face severe penalties. Organizations should also have plans in place to recover from security breaches when they occur. Consumers have the right for their data to be available in a portable 'commonly use and machine readable' format. They also have the right to transfer their data to a different provider [96], [98], [101], [102].

## *B. Technical Aspect*

### *1) Patient Centric Approach*

It is a community of healthcare systems where patients can store, access, update, and share their health data [103]. Patient centric offers secure storage and administration of patients EHRs, which could be utilized for disease treatment, research, and other applications. Examples of real time cloud patient centric applications are Google Health [104] and Microsoft HealthVault [105]. Both applications implement a centralized architecture where patients store and update health data in EHR system, and patients have full control over their data [77]. Since patient PHR stored in the cloud or at third party, there have been wide privacy issues because patient private health data could be used by third-party servers or unauthorized users. To assure the patients' privacy and to enhance security, it is highly recommended to encrypt patient data before outsourcing [106]. Encrypting data takes time and may affect performance.

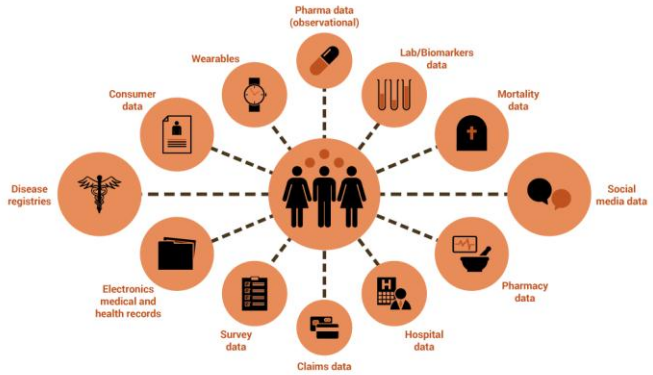


**Figure 4.** Information centric healthcare model [107].

The task of aggregating health records from different sources in a single repository is a complex task since the aggregator needs to use different standards and protocols to guarantee interoperability between different stakeholders. On the other hand, the use of different standards makes it hard to secure the application, and makes it prone to security breaches. The problem with the patient centric approach to solving the security problem is the contradicting requirements. Giving the power to the patients to decide who can access their records might prevent a doctor from accessing those records in case of an emergency. Applying multilayer security measures to guarantee that only authorized users can access the system might slow the system down and collides with the doctors need for fast and quick systems. Added security measures will negatively affect the user experience. The fundamental need for different parties to access the patient data makes the patient data more vulnerable to security breaches. Giving the patient the ability to edit his own medical records might collide with the doctor's requirement to guarantee data originality [108], [109].

*2) Encryption Techniques*

Cloud computing and the widespread connectivity, have increased the risk of data breaches. Health data is highly sensitive and safeguarding this data is a high priority for individuals, healthcare providers, and cloud services providers. Encryption is considered an important part of the security policy of organizations and service providers because it can circumvent intruders gaining value from data. Encryption is a technique that is used to scramble cleartext data into ciphertext with a key. The key is used later by authorized party to decode data to the original form. Encryption uses a computer algorithm to decode data and generate the key where knowing or guessing the key is highly difficult. Ciphertext (encrypted data) is considered more secure from the clear text data and it prevents unauthorized users from obtaining a value or meaning from accessing the data. In cloud computing, encryption must be considered during data in motion, data at storage, and during data deletion [110].

Encrypting of data in transit is the process of encrypting data at one location, transferring it over the network, then decoding data at the cloud. It became an important process because unauthorized eyes could have access to the data on the way, causing data integrity issue (data could be modified or stolen during transfer). The Transport Layer Security (TLS) has been utilized to secure communication between web applications. TLS reserves an encrypted channel to establish negotiations between senders and receivers to send the cipher, then transfer the key using public key cryptography [111].

In cloud computing, sensitive data-in-rest suffers many threats that can cause data leakage. Self Encrypting Drive (SED) is a hard drive that contains an internal circuit that encrypts and decrypt all data automatically, and use authentication procedure when the host system is powered on [110]. Encryption key management is crucial for data-in-rest encryption, therefore, it is highly recommended to maintain control of all keys, store keys externally, and maintain transparent encryption to the users [112]. The goal of secure-data-deletion encryption is to protect data deletion against expert attackers so that securely deleted data is not recoverable. If the attacker has a backup version of deleted encrypted data, then the system admin and users must guarantee that the corresponding decoding key is also strictly deleted to prevent attacker from decoding data thereafter [113].

## CASE STUDY: MICROSOFT HEALTHVAULT VS GOOGLE HEALTH

Online internet based PHRs applications are defined as "*electronic application through which individuals can access, manage and share their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment*" [114]. Unlike EHRs that are institution controlled, PHR are patient controlled. The main idea is to aggregate the patient's health records in a single secure repository that can be accessed by different parties like patients, hospitals, doctors, and insurance companies. It is also clear from the definition that the viability of this technology is highly dependent on the availability of "privacy", "security", and "confidentiality". There exists many PHR applications with different designs, architectures, and user interfaces like Google Health [104], Microsoft HealthVault [105], Apple's Healthkit [115], World Medical Card [116], and Dossia [117]. The wide adoption of this technology is hindered by the fact that people do not trust corporations like Google and Microsoft with their personal health data. They worry that those corporations will share their data with employers and insurance companies, they also worry that their data will show on internet searches.

In this section, two online web-based applications particularly Google Health and Microsoft HealthVault are compared. The comparison focuses particularly on security, privacy, and trust issues. Both applications were launched in 2008, and they both claim that online PHRs are as secure as online banking, they also claim that electronic records are more secure than paper records because there are minimum human interferences. To gain consumer trust, and to avoid security disasters both applications are patient controlled, meaning that the application cannot retrieve or share a patient medical

record without the patient explicit permission. It is hard to believe that both applications are not going to use patient data to create targeted advertisements since the only way both applications can make money is by selling advertisements next to search results [118].

Google Health and Microsoft HealthVault have lots of similarities and few differences. Both entities are patient controlled, they both claim data portability, and the business model for both applications is unclear [118]. Both Google Health and Microsoft HealthVault embraced open standards, they both use HL7 Simple Object Access Protocol (SOAP) to facilitate web-services interoperability, and the Continuity of Care Record (CCR) to facilitate data exchange. The use of open standards makes both applications prone to threats and attacks [108], [109], [118]. In addition, both applications are not considered a "covered entity" according to HIPAA standards suggesting that HIPAA privacy laws do not apply. The goal of both applications is to build a sizable network, the bigger the network, the higher the value of the network, and the more it is vulnerable to attacks [108], [109], [118].

Table 1 summarizes the state of Google Health and Microsoft HealthVault with respect to different features like libraries, authentication, security, data access, data modification, and data messages. Microsoft HealthVault is more secure because it uses closed source libraries. Microsoft HealthVault uses .NET SDK where Google Health Java, .NET, Python, and PHP libraries. Google Health also used the Direct Project open protocol for the exchange of health data. Regarding Authentication, Google Health allows web and client login, whereas in Microsoft HealthVault client login is possible through web login. Microsoft HealthVault obligates security certificates, whereas Google Health uses security certificates at web login. Microsoft Health Vault allows Create, Read, Update, and Delete (CRUD) operations, whereas Google Health have limited data access, it only allows Read and Write or Write only modes. With respect to data modification, Microsoft HealthVault allows direct editing and modification of data. On the other hand, every Google Health modification is packed into a notice to ensure that patients are aware of every change made to their account [109], [118].

**Table I:** Google Health vs. Microsoft Vault Health [108].

| | **Google Health** | **MS HealthVault** |
|---|---|---|
| **Libraries** | Open source | Closed source |
| **Authentication** | Web and client login | Web login only |
| **Security** | Security certificates only by using Web-Login | Security certifications are obligated |
| **Data Access** | READ+WRITE or WRITE only | CRUD operations |
| **Data Modification** | Every object sent to Google treated as a notice | Direct editing of data |
| **Data Messages** | Malformed XML string | XML compliant to w3cDom |

Security, privacy, and trust issues seems to be the main reasons behind the failure of Google Health and the success of Microsoft HealthVault. Google Health used a public cloud where Microsoft Vault Health used a private cloud as a result Google Health was more vulnerable to attacks. The fact that Google Health uses open and versatile source makes it easy to develop applications but makes it more prone to security threats. Google Health is less flexible, the user has less control over his data, and there are restrictions over data access making it more secure and less convenient. Google Health was the victim of contradicting requirements, it failed to find a good balance between security and convenience, and customers were less inclined to use it.

## CONCLUSION

Security is one of the main problems that hinders the fast adoption of the cloud computing technology in the healthcare industry. The strengths and benefits of cloud computing far exceeds its dangers and threats. Security requirements are increasingly difficult to meet without a significant investment in infrastructure and manpower. The dilemma is that security is negatively proportional to consumer convenience. In other words, the more sophisticated the security measures, the less comfortable the consumers, and as a result, they are going to be less inclined to use the cloud service. In this paper, we found that the surveyed solutions are not holistic in nature, those approaches partially solve the security challenge. Most of those solutions address part of the problem, and they failed to balance all contradicting security requirements. The problem is that a gain obtained in one dimension causes a loss in another dimension. In the future, we will propose a holistic solution that attempts to balance all contradicting requirements.

Migration of an organization data to the cloud is a strategic and complex decision. Before moving data into the cloud, the security challenges should be mitigated. A good cloud service provider should monitor the protected health data life-cycle. Before selecting a cloud service provider, different questions should be asked like: is the provider ISO/IEC 72001 certified? is the provider compliant with the security and privacy regulatory acts? is the provider staff trained on risk and crisis management? whether the provider performs periodic security checks? is the service provider willing to sign a strong HIPAA Business Associate Agreement (BAA) that contains severe punishment in case of terms violation. Different security measures like firewalls, intrusion detection, and the type of encryption and authentication techniques should be also checked.

**REFERENCES**

[1] European Network Information Security Agency, "An SME perspective on Cloud Computing." 2009.

[2] A. M.-H. Kuo, "Opportunities and challenges of cloud computing to improve health care services," *J. Med. Internet Res.*, vol. 13, no. 3, 2011.

[3] Y. Levy and T. J. Ellis, "A systems approach to conduct an effective literature review in support of information systems research.," *Informing Sci.*, vol. 9, 2006.

[4] S. Keele and others, "Guidelines for performing systematic literature reviews in software engineering," in *Technical report, Ver. 2.3 EBSE Technical Report. EBSE*, sn, 2007.

[5] P. Mell and T. Grance, "The NIST definition of cloud computing [Recommendations of the National Institute of Standards and Technology-Special Publication 800-145]," *Washingt. DC NIST. Recuper. http//csrc. nist. gov/publications/nistpubs/800-145/SP800-145. pdf*, 2011.

[6] D. Sinanc and S. Sagiroglu, "A review on cloud security," in *Proceedings of the 6th International Conference on Security of Information and Networks*, 2013, pp. 321–325.

[7] K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," in *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications*, 2011, p. 12.

[8] D. A. B. Fernandes, L. F. B. Soares, J. V Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," *Int. J. Inf. Secur.*, vol. 13, no. 2, pp. 113–170, 2014.

[9] Salesforce, "Salesforce." 2017.

[10] Microsoft, "Office 365." 2017.

[11] Cloudfoundry, "Cloudfoundry." 2017.

[12] Amazon, "Amazon EC2." 2017.

[13] P. Banerjee *et al.*, "Everything as a service: Powering the new information economy," *Computer (Long. Beach. Calif).*, vol. 44, no. 3, pp. 36–43, 2011.

[14] B. P. Rimal, A. Jukan, D. Katsaros, and Y. Goeleven, "Architectural requirements for cloud computing systems: an enterprise cloud approach," *J. Grid Comput.*, vol. 9, no. 1, pp. 3–26, 2011.

[15] VMWare, "VMWare." 2017.

[16] Dropbox, "Dropbox." 2017.

[17] Microsoft, "Microsoft Azure," 2017. [Online]. Available: https://azure.microsoft.com.

[18] Rackspace, "Rackspace." 2017.

[19] "NYSE Capital Markets Community Platform." 2017.

[20] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "e-Health cloud: opportunities and challenges," *Futur. Internet*, vol. 4, no. 3, pp. 621–645, 2012.

[21] N. Dong, H. Jonker, and J. Pang, "Challenges in eHealth: From Enabling to Enforcing Privacy.," in *FHIES*, 2011, pp. 195–206.

[22] S. Allen, "Cloud Computing and Health Care Security," *Cloud Comput. Journal. Retrieved from*, 2011.

[23] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, and G. Müller, "Aspects of privacy for electronic health records," *Int. J. Med. Inform.*, vol. 80, no. 2, pp. e26--e31, 2011.

[24] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds," *IEEE J. Biomed. Heal. Informatics*, vol. 18, no. 4, pp. 1431–1441, 2014.

[25] ANSI, "TS 18308 health informatics-requirements for an electronic health record architecture," *ISO*, 2003.

[26] US Department of Health & Human Services (HHS), "Health Information Privacy." 2005.

[27] R. Bakker, B. Barber, R. Tervo-Pellikka, and A. Treacher, "Communicating health information in an insecure world," in *Proceedings of the Helsinki Working Conference*, 1995, vol. 43, no. 1, p. 2.

[28] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Comput. Surv.*, vol. 45, no. 1, p. 3, 2012.

[29] C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu, "From security to assurance in the cloud: a survey," *ACM Comput. Surv.*, vol. 48, no. 1, p. 2, 2015.

[30] A. Ibrahim, B. Mahmood, and M. Singhal, "A secure framework for sharing Electronic Health Records over Clouds," in *Serious Games and Applications for Health (SeGAH), 2016 IEEE International Conference on*, 2016, pp. 1–8.

[31] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, 2013.

[32] J. Andress, *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress, 2014.

[33] P. Metri and G. Sarote, "Privacy issues and challenges in cloud computing," *Int. J. Adv. Eng. Sci. Technol.*, vol. 5, no. 1, pp. 5–6, 2011.

[34] Accountability Act, "Health insurance portability and accountability act of 1996," *Public Law*, vol. 104, p. 191, 1996.

[35] P. Duquenoy, N. M. Mekawie, and M. Springett, "Patients, trust and ethics in information privacy in

eHealth," in *eHealth: Legal, Ethical and Governance Challenges*, Springer, 2013, pp. 275–295.

[36] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 2, pp. 843–859, 2013.

[37] M. Scholl *et al.*, "An introductory resource guide for implementing the health insurance portability and accountability act (HIPAA) security rule (NIST Special Publication 800-66, rev. 1). Gaithersburg, MD: Computer Security Division," *Inf. Technol. Lab. Natl. Inst. Stand. Technol. Retrieved from htt p//csrc. nist. gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1. pdf*, 2008.

[38] D. Blough, M. Ahamad, L. Liu, and P. Chopra, "MedVault: Ensuring security and privacy for electronic medical records," in *NSF CyberTrust Principal Investigators Meeting. Online at http://www. cs. yale. edu/cybertrust08/posters/posters/158 medvault poster CT08. pdf*, 2008.

[39] Washington Electronic Authentication Act, "Revised Code of Washington," *Vol RCW*, vol. 70, no. 10, 1992.

[40] A. McCullagh and W. Caelli, "Non-repudiation in the digital environment," *First Monday*, vol. 5, no. 8, 2000.

[41] Integrating the Healthcare Enterprise, "IHE Profiles." 2017.

[42] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer (Long. Beach. Calif).*, vol. 29, no. 2, pp. 38–47, 1996.

[43] R. S. Sandhu, "Role-based access control," 1997.

[44] A. Mohan and D. M. Blough, "An attribute-based authorization policy framework with dynamic conflict resolution," in *Proceedings of the 9th Symposium on Identity and Trust on the Internet*, 2010, pp. 37–50.

[45] M. Hagner, "Security infrastructure and national patent summary," in *Tromso Telemedicine and eHealth Conference*, 2007.

[46] C. G. Schermer and Brockelman, "HITECH Act expands HIPAA privacy and security rules." 2009.

[47] HIPAA Survival Guide, "HITECH Act Summary," *Retrieved August*, vol. 28, p. 2012, 2012.

[48] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research," *Int. J. Internet Enterp. Manag.*, vol. 6, no. 4, pp. 279–314, 2010.

[49] P. Samarati, "Protecting respondents identities in microdata release," *IEEE Trans. Knowl. Data Eng.*, vol. 13, no. 6, pp. 1010–1027, 2001.

[50] B. Malin, E. Airoldi, and others, "Confidentiality preserving audits of electronic medical record access," *Stud. Health Technol. Inform.*, vol. 129, no. 1, p. 320, 2007.

[51] J. Domingo-Ferrer, A. Martinez-Ballesté, J. M. Mateo-Sanz, and F. Sebé, "Efficient multivariate data-oriented microaggregation," *VLDB Journal—The Int. J. Very Large Data Bases*, vol. 15, no. 4, pp. 355–369, 2006.

[52] K. Muralidhar and R. Sarathy, "An enhanced data perturbation approach for small data sets," *Decis. Sci.*, vol. 36, no. 3, pp. 513–529, 2005.

[53] A. Pfitzmann and M. Hansen, "Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology," 2005.

[54] A. Behl and K. Behl, "An analysis of cloud computing security issues," in *Information and Communication Technologies (WICT), 2012 World Congress on*, 2012, pp. 109–114.

[55] A. Behl, "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," in *Information and communication technologies (WICT), 2011 world congress on*, 2011, pp. 217–222.

[56] C. V Wright, L. Ballard, S. E. Coull, F. Monrose, and G. M. Masson, "Uncovering spoken phrases in encrypted voice over IP conversations," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 4, p. 35, 2010.

[57] C. V Wright, S. E. Coull, and F. Monrose, "Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis.," in *NDSS*, 2009, vol. 9.

[58] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting your daily in-home activity information from a wireless snooping attack," in *Proceedings of the 10th international conference on Ubiquitous computing*, 2008, pp. 202–211.

[59] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography," *IEEE Access*, 2017.

[60] N. Koblitz and A. Menezes, "Pairing-based cryptography at high security levels," *Lect. notes Comput. Sci.*, vol. 3796, p. 13, 2005.

[61] J. Voris, J. Jermyn, A. D. Keromytis, and S. J. Stolfo, "Bait and snitch: Defending computer systems with decoys," in *Proceedings of the cyber infrastructure protection conference, Strategic Studies Institute, September*, 2013.

[62] S. P. KAREKAR and S. M. VAIDYA, "Perspective of Decoy Technique using Mobile Fog Computing with Effect to Wireless Environment," 2015.

[63] J. Shropshire, "Extending the cloud with fog: Security challenges & opportunities," 2014.

[64] K. Manreet and B. Monika, "Fog computing providing data security: a review," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 6, pp. 832–834, 2014.

[65] M. Marwan, A. Kartit, and H. Ouahmane, "Protecting medical data in cloud storage using fault-tolerance mechanism," in *Proceedings of the 2017 International Conference on Smart Digital Environment*, 2017, pp. 214–219.

[66] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[67] A. Galletta, L. Bonanno, A. Celesti, S. Marino, P. Bramanti, and M. Villari, "An approach to share MRI data over the Cloud preserving patients' privacy," in *Computers and Communications (ISCC), 2017 IEEE Symposium on*, 2017, pp. 94–99.

[68] E. Alexander and others, "Privacy-Aware Set-Valued Data Publishing on Cloud for Personal Healthcare Records," in *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Springer, 2017, pp. 323–334.

[69] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *Int. J. Uncertainty, Fuzziness Knowledge-Based Syst.*, vol. 10, no. 5, pp. 571–588, 2002.

[70] M. Terrovitis, N. Mamoulis, and P. Kalnis, "Privacy-preserving anonymization of set-valued data," *Proc. VLDB Endow.*, vol. 1, no. 1, pp. 115–125, 2008.

[71] M. B. Smithamol and S. Rajeswari, "Hybrid Solution for Privacy-Preserving Access Control for Healthcare Data," *Adv. Electr. Comput. Eng.*, vol. 17, no. 2, pp. 31–38, 2017.

[72] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 89–98.

[73] S. Sneha and P. Asha, "Privacy preserving on E-Health records based on Anonymization technique," *Glob. J. Pure Appl. Math.*, vol. 13, no. 7, pp. 3367–3380, 2017.

[74] B. Dhivya, S. P. Siqqiue Ibrahim, and R. Kirubakaran, "Hybrid Cryptographic Access Control for Cloud based Electronic Health Records Systems," 2017.

[75] K. Shah and V. Prasad, "Security for Healthcare Data on Cloud," 2017.

[76] S. Supriya and S. Padaki, "Data Security and Privacy Challenges in Adopting Solutions for IOT," in *Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on*, 2016, pp. 410–415.

[77] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, 2010, pp. 268–275.

[78] H. Löhr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in *Proceedings of the 1st ACM International Health Informatics Symposium*, 2010, pp. 220–229.

[79] J. L. Griffin, T. Jaeger, R. Perez, R. Sailer, L. Van Doorn, and R. Cáceres, "Trusted virtual domains: Toward secure distributed services," in *Proceedings of the 1st IEEE Workshop on Hot Topics in System Dependability (HotDep'05)*, 2005, pp. 12–17.

[80] US Department of Health & Human Services (HHS), "Summary of the HIPAA security rule," *Retrieved December*, vol. 5, p. 2016, 2013.

[81] US Department of Health & Human Services (HHS), "Summary of the HIPAA privacy rule," *Retrieved December*, vol. 5, p. 2016, 2015.

[82] K. J. Cios and G. W. Moore, "Uniqueness of medical data mining," *Artif. Intell. Med.*, vol. 26, no. 1, pp. 1–24, 2002.

[83] US Department of Health & Human Services (HHS), "Methods for De-identification of PHI." 2010.

[84] S. E. White, "A review of big data in health care: challenges and opportunities," *Open Access Bioinformatics*, vol. 6, pp. 13–18, 2014.

[85] O. Tene and J. Polonetsky, "Privacy in the age of big data: a time for big decisions," *Stan. L. Rev. Online*, vol. 64, p. 63, 2011.

[86] M. A. Ottom, "Big Data in Healthcare: Review and Open Research Issues," *Jordanian J. Comput. Inf. Technol.*, 2017.

[87] D. Blumenthal, "Launching hitech," *N Engl J Med*, vol. 2010, no. 362, pp. 382–385, 2010.

[88] HealthITgov, "Nationwide Health Information Network (NwHIN)." 2017.

[89] "ISO/IEC 27000-Series Standard," 2017. [Online]. Available: http://www.iso27001security.com/html/27000.html.

[90] "International Organization for Standardization (ISO)." 1947.

[91] "International Electrotechnical Commission (IEC)," 2017. [Online]. Available: https://en.wikipedia.org/wiki/International_Electrotechnical_Commission.

[92] "ISO/IEC 27001 (Information Technology: Security Techniques, Systems Requirements)." 2016.

[93] "ISO/IEC 27002 (Information Technology: Security Techniques - Code of Practice for Information Security Management)," 2016. [Online]. Available: http://www.iso27001security.com/html/27002.html.

[94] "ISO/IEC 27002 code of practice." 2016.

[95] R. Gomes and L. V. Lapão, "The adoption of IT security standards in a healthcare environment," *Stud. Health Technol. Inform.*, vol. 136, p. 765, 2008.

[96] "EU General Data Protection Regulation (GDPR)," 2017. [Online]. Available: http://www.eugdpr.org/.

[97] S. Gibbs, "European parliament approves tougher data privacy rules." 2016.

[98] "General Data Protection Regulation." 2016.

[99] IT Governance, "EU General Data Protection Regulation Infographic." 2017.

[100] H. Wilson, "European data protection laws are changing." 2017.

[101] IT Governance, "EU General Data Protection Regulation (GDPR)." 2017.

[102] J. M. Victor, "The EU general data protection regulation: Toward a property regime for protecting data privacy," *Yale LJ*, vol. 123, p. 513, 2013.

[103] M. J. Minniti, T. R. Blue, D. Freed, and S. Ballen, "Patient-interactive healthcare management, a model for achieving patient experience excellence," in *Healthcare Information Management Systems*, Springer, 2016, pp. 257–281.

[104] Google, "Google Health," 2011. [Online]. Available: https://en.wikipedia.org/wiki/Google_Health.

[105] Microsoft, "Microsoft HealthVault." 2007.

[106] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, 2013.

[107] Privacy Analytics Inc., "Patient-Level Data." 2017.

[108] A. Sunyaev, "Evaluation of Microsoft HealthVault and Google Health personal health records," *Health Technol. (Berl).*, vol. 3, no. 1, pp. 3–10, 2013.

[109] A. Sunyaev, D. Chornyi, C. Mauro, and H. Krcmar, "Evaluation framework for personal health records: Microsoft HealthVault vs. Google Health," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, 2010, pp. 1–10.

[110] L. Coyne *et al.*, *Ibm private, public, and hybrid cloud storage solutions*. IBM Redbooks, 2017.

[111] M. G. Solomon, *Security Strategies in Windows Platforms and Applications*. Jones & Bartlett Publishers, 2013.

[112] K. Scarfone, "The True Story of Data-At-Rest Encryption & the Cloud," 2015.

[113] J. Reardon, H. Ritzdorf, D. Basin, and S. Capkun, "Secure data deletion from persistent media," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 271–284.

[114] Health Personal Health Working Group, "The Personal Health Working Group: final report," *Markel Found. July*, vol. 1, p. 2003, 2003.

[115] Apple, "Apple Healthkit." 2017.

[116] "World Medical Card." 2017.

[117] Dossia, "Dossia." 2017.

[118] Vince Kuraitis, "A First Comparison of Google Health and MS HealthVault." 2008.