A HOLISTIC INSIGHT INTO THE PRIVACY & SECURITY OF CLOUD-BASED COMPUTING APPROACH ON HEALTHCARE INFORMATION MANAGEMENT SYSTEMS IN THE UNITED STATES – A GROUNDED THEORY APPROACH

Foday Junior Conteh

Marymount University, Arlington, Virginia

ABSTRACT

Cloud computing (CC) represents a significant technological advancement in the United States (U.S.) healthcare. Despite its advantages like reduced costs, scalability, resource sharing, and high availability, CC raises concerns, especially in privacy and security. This study employs Grounded Theory methodology to delve into these concerns within cloud-based Healthcare Information Management Systems (HIMS) in the U.S., which operates under stringent patient privacy and security laws. The research focuses on healthcare organizations' strategies to mitigate these challenges. In-depth interviews and document analysis, conducted using a qualitative research strategy, will gather data from healthcare professionals and Information Technology (I.T.) specialists interacting with cloud-based HIMS. Through thematic analysis and constant comparison, the research will construct a theoretical framework showcasing CC's impact on HIMS privacy and security. This framework will establish a basis for subsequent research to improve U.S. healthcare delivery by directing organizations to adopt and implement cloud-based HIMS compliant with U.S. data privacy regulations.

KEYWORDS

Cloud Computing, Privacy, Security, Health Information Management Systems (HIMS), Grounded Theory Methodology

1. INTRODUCTION

Cloud computing (CC) has become increasingly prevalent among organizations of all sizes for hosting critical applications and storing sensitive data. While CC presents a revolutionary shift from traditional on-premises security, concerns about its security uncertainties have influenced its adoption rate, especially in critical infrastructure sectors like healthcare. Notably, Gartner's Cloud Shift research (2019-2025) predicts a substantial increase in cloud adoption, with public cloud solutions poised to constitute over half of I.T. spending in key segments by 2025 [1]. The transition from traditional to cloud infrastructure is evident in the healthcare sector. A forecast by [2] projects a surge in the global healthcare cloud infrastructure market, growing from US$39.7 billion in 2020 to over US$157.8 billion by 2030. Integrating digital technologies such as

David C. Wyld et al. (Eds): CNSA, DMDB, NIAI, ICCIoT, AIAP -2024
pp. 01-31, 2024. CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.140101

Artificial Intelligence (A.I.), CC, the internet, and data analytics in healthcare settings drives this growth.

This study will adopt a grounded theory research design to develop insights into the privacy and security impacts of CC on HIMS. Research by [3] suggests that CC fosters coordination, communication, and collaboration within the healthcare sector, leading to significant improvements in care delivery. Cloud-based HIMS adoption is expected to revolutionize healthcare delivery, as demonstrated by studies like [4]. However, the rapid adoption of CC in healthcare, a sector with a paramount emphasis on data security due to regulations like the Health Insurance Portability and Accountability Act (HIPAA), raises critical questions about its implications on patient data security and privacy. This research offers comprehensive insights into these questions, evaluating CC's cybersecurity benefits and challenges compared to traditional on-premises solutions.

2. BACKGROUND OF THE STUDY

Recent research has extensively explored cloud computing (CC) within the healthcare sector, focusing on its impact on patient care delivery and associated data security and privacy concerns. Mehrtak et al. [5] highlight the simplification of user collaboration, reduction in infrastructure and service costs, and improvements in agility, scalability, and flexibility as key advantages of adopting cloud technology in healthcare. They also note how CC transforms the provision of high-quality, cost-effective care by healthcare professionals, including nurses and doctors, as well as hospitals and clinics. However, they caution about the potential drawbacks, particularly in confidentiality, privacy, and service costs, which make healthcare organizations hesitant about CC utilization.

Mehraeen et al. [6] addressed challenges related to interoperability between cloud-hosted information systems and legacy applications within healthcare organizations. Their study emphasizes that while migrating to the cloud offers numerous benefits, it does not negate the challenges associated with healthcare data privacy, transparency, risk management, compliance, and information security.

Maslin and Rahimli [7] conducted a SWOT analysis to investigate the adoption of CC in healthcare. Their findings suggested that, despite the advantages of cost reduction, enhanced storage capacity, and improved collaboration among primary care providers, significant risks, including data security and compliance issues, persist. Their research particularly pointed out the concerns related to cloud security in patient care data.

Reference [8] explored how emerging CC technology contributes to healthcare provision, examining its application across various healthcare segments such as primary patient care services, medical research organizations, and pharmaceutical companies. The study highlighted the development of a cloud-based clinical information system, "Collaborative Care Solution," by IBM and ActiveHealth Management, emphasizing its role in facilitating access to primary care physicians and health records. However, [8] also acknowledged the security risks, service interruptions, and reliance on single cloud service providers as deterrents to CC adoption.

Abrar et al. [9] focused on the risk analysis of cloud sourcing in healthcare and public health. Their study found that the central principle of CC is the shared security responsibility model, contrasting with the full responsibility model in on-premises systems. They concluded that while CC is seen as a quick fix to security vulnerabilities, its adoption in healthcare has been hampered due to these significant risk concerns.

The proposed research aims to assess and evaluate cybersecurity risks in cloud-based HIMS, particularly concerning patient data security and privacy. This will involve participant interviews and a review of existing literature identifying security risks primarily associated with cloud storage data breaches. These breaches are often attributed to misconfigurations in cloud services and a lack of understanding among healthcare organizations of their shared security responsibilities with Cloud Service Providers (CSPs).

The potential of cloud-based HIMS in enhancing healthcare delivery has increased interest, particularly regarding quality, accessibility, and efficiency. Such systems facilitate the secure and convenient remote storage, administration, and retrieval of patient records. However, as cloud-based HIMS gained popularity, concerns regarding the privacy and security of healthcare information stored in the cloud have escalated.

The Cloud Maturity Model (CMM), described by SEAGATE [10], offers a structured approach for organizations to assess their readiness for cloud migration and optimize cloud-based services. This model will be instrumental in the current study for evaluating the cloud adoption readiness of healthcare organizations, focusing on managing patient data privacy and security in the cloud.

In conclusion, the study aims to provide healthcare organizations with recommendations and guidelines to effectively determine their cloud roadmap and prepare healthcare personnel for managing patient data when hosted in the cloud.

2.1. Problem Statement

The healthcare sector, recognized as a critical infrastructure, faces unique challenges in protecting patient data, especially with the increasing adoption of CC. Reports by [11] and [12] highlight the growing market for healthcare cloud infrastructure and the rising incidents of healthcare data breaches. The need for secure and compliant healthcare technology platforms is more pressing than ever, with the digitization of healthcare services like Electronic Health Records (EHR) introducing benefits and security threats [13]. The healthcare sector's reliance on EHR and the digitization of healthcare services compels a rigorous examination of the privacy and security implications of CC. This research aims to provide a comprehensive analysis of these implications, contributing significantly to the field by informing healthcare organizations on effective CC strategies that ensure the security and privacy of patient data.

2.2. Research Question

This study will employ a qualitative grounded theory design methodology to gain insight into the impact of CC on the privacy and security of HIMS in patients' Protected Health Information (PHI) in the U.S. The research question (RQ1) is:

- How has the cloud-based computing approach to HIMS improved the privacy and security of patients' PHI in the U.S.?

2.3. Significance

This study is of utmost importance as it addresses the critical need for robust privacy and security measures in HIMS containing sensitive patient information. With the rising incidence of data breaches in healthcare, as reported by [12] and [14], understanding the implications of CC on

patient data confidentiality and security is crucial. By exploring CC adoption in healthcare, this research aims to guide organizations in enhancing their cybersecurity measures, ultimately contributing to safeguarding patient well-being and trust in the healthcare system.

3. RELATED WORK

The cloud-based computing approach has emerged as a prevalent technological solution for organizations, irrespective of size, scope, and location. This technology has provided a platform that transcends the traditional limitations of brick-and-mortar organizations, driving its rapid adoption and implementation across a broad spectrum of business sectors. Organizations face a dual scenario in adopting and implementing CC: either overhaul their legacy on-premises applications and data services in favor of CC or integrate these existing systems with CC, making it central to all mission-critical applications and database services operations.

The adoption of CC within the U.S. healthcare sector is particularly noteworthy, classified as part of the country's critical infrastructures. This sector utilizes CC to host mission-critical applications and manage workloads that include sensitive patient care information for processing and data storage. The technological benefits of CC, such as its virtualized web service enabling constant accessibility, along with features supporting scalability, elasticity, and high availability of enterprise infrastructure, make it an attractive technology for the healthcare industry. By adopting CC, the healthcare sector can meet increasing patient care demands, including telehealth services, and reduce costs associated with managing and storing the growing volume of patient data. Consequently, CC's adoption in healthcare presents an ideal case study for researching the impact on patient data privacy and security.

3.1. Shared Responsibility in Cloud Computing: A Thematic Exploration

Organizations transitioning to cloud computing as an alternative or primary platform for hosting workloads (e.g., applications, database services) encounter challenges securing cloud computing (CC) solutions and architectures. This study, however, focuses on the impacts of adopting cloud privacy and security within HIMS and does not delve into detailed discussions of cloud architecture and infrastructure security.

A critical aspect of CC security and privacy is understanding the security responsibilities of cloud consumers relative to the chosen cloud deployment and service model. Cloud Service Providers (CSPs) are obligated to secure the cloud's underlying infrastructure and resources, which vary based on the service and deployment models adopted by the consumer. An essential concept in CC security, the shared security responsibility model, is discussed.

The shared responsibility model outlines a framework for cloud security, depicting the CSP's duty to secure the cloud infrastructure and the cloud customer's responsibility for securing contents within the cloud, including services, applications, and data. Many cloud consumers adopt CC with a limited understanding of their security responsibilities, which is critical for ensuring continuous data confidentiality, integrity, and availability. This model educates adopters on securing cloud workloads and addressing CC security and privacy challenges akin to traditional on-premises data and application security.

For example, in on-premises data centers, businesses ensure data security at rest and in transit, with applications and database services shielded behind firewalls without direct public access. This data security and defense-in-depth concept is replicable in the cloud, provided a robust understanding of the shared security responsibility model exists.

In summary, unlike traditional on-premises setups, cloud service models assign the sole responsibility for all underlying physical infrastructure, from physical networks to hypervisors to the CSP. The shared responsibility between the CSP and the cloud customer commences at the virtualized services and resources level, such as virtual networks built atop the cloud platform hypervisors. The cloud customer is tasked with defining logical networks within the cloud environment and controlling network traffic to their subnets and virtual machines hosting applications and databases. Paramount is the cloud customers' responsibility to ensure that administrators, engineers, and personnel interacting with cloud services possess the necessary skills and permissions to meet the organization's security, privacy, and business requirements.

Despite the growing adoption of cloud technology for business innovation, some industries and sectors are slow to embrace it, often due to a potential cloud skills gap. In an era of increasing interconnectedness, data volume is escalating rapidly. Gartner predicts that the number of Internet of Things (IoT) devices will double approximately every five years, projecting over 15 billion IoT devices linked to business networks by 2029, making CC crucial for leveraging analytics, such as predictive modeling [15]. Many businesses face challenges due to a lack of necessary cloud-based skills among their employees, hindering cloud development and the swift adoption of new technologies, impacting their digital transformation initiatives [15].

Unfortunately, CC adopters' cloud skills shortage has contributed to increased data breaches and malware attacks against cloud-hosted technologies, primarily due to improperly configured cloud resources and services. Misconfigurations in the Cloud have escalated over the years. For instance, the number of exposed data records rose by 80% from 2018 to 2019, along with the costs associated with managing the damage [16]. Reference [16] reports that in 2018, about 11.8 billion cloud records were exposed, costing organizations approximately $1.76 trillion, and this figure rose to 21.2 billion records in 2019, with costs soaring to $3.18 trillion.

As cloud service adoption increases, so does the likelihood of cloud misconfigurations, a leading challenge in cloud security and data privacy. Understanding the shared responsibility model can aid cloud customers in establishing a standard security baseline for data security and privacy in the cloud.

This study will explore the privacy and security impact of cloud-based technology adoption in the healthcare sector. It aims to analyze cloud customers' comprehension of the shared responsibility model concerning privacy and security impacts on healthcare organizations' cloud-based information management systems. Before adopting cloud computing for database and application hosting, organizations must define business requirements for cloud adoption, encompassing an understanding of CC technology in terms of cost, usage benefits, and performance metrics, including data security, privacy, and productivity.

A comprehensive cost and usage benefit analysis is critical before adopting CC technology, encompassing all cloud adoption variables, such as cost, accessibility, storage features, data security, and privacy. The study will subsequently discuss theories to define the roadmap for adopting CC as a service in the healthcare sector and the associated implications and challenges concerning cloud privacy and security.

3.2. Healthcare Cloud Adoption: Insight from Grounded Theory and TOE Framework

Reference [17] explains that Grounded Theory has been employed in information technology and management research, including studies on CC. This inductive qualitative research methodology posits that theories should emerge from data, ensuring that the developed theory aligns with empirical findings [18]. Fernández and Lehmann [19] noted the absence of existing theories for emerging phenomena, emphasizing the significance of Grounded Theory in exploring uncharted territories in research. Grounded Theory's inductive, process-based strategies are instrumental in constructing and extending knowledge, particularly in areas where established theories are inadequate [17]. This study expands upon previous research on cloud-based adoption in healthcare, addressing their limitations and filling the existing knowledge gaps.

Additionally, the Technology Organization-Environment (TOE) framework will be a critical component of this research, aiding in identifying relevant factors and variables influencing CC adoption in healthcare organizations. Conceived by Tornatzky and Fleischer, the TOE framework is a multi-perspective model considering technological, organizational, and environmental factors impacting the adoption of technological innovation [20], [21]. Various studies have applied this framework to analyze factors influencing new information technology innovations [21]. The scalability, flexibility, and cost-effectiveness of cloud technology, coupled with organizational and environmental factors, play a pivotal role in its adoption in healthcare.

The healthcare industry's fragmented service delivery, driven by complex and often non-integrated information infrastructures, highlights the need for cloud technology [22]. Adoption of CC enables access to large-scale computing resources and advanced analytic services, essential for addressing the industry's challenges, including resource limitations, care delivery, administrative burdens, and availability of critical services [22], [23]. Understanding the factors influencing the relationship between cloud adoption and I.T. department efficiency is crucial for providing healthcare organizations with a viable cloud adoption roadmap [23].

The significance of digital health technology is increasingly evident, as shown by the rise in the use of digital health tools among physicians, as reported by [24]. Integrating patient data into healthcare outcomes and cost-reduction strategies compels ethical and secure data management. Cloud-based technologies offer robust data collection, processing, transmission, and storage solutions. However, selecting CSPs experienced in healthcare-specific regulations, such as HIPAA, is critical [25].

Before adopting cloud services, healthcare organizations must consider various regulatory aspects, ensuring compliance with existing regulations, such as HIPAA, for cloud-based patient healthcare solutions [26]. The Grounded Theory approach, focusing on action and process analyses [27], will enable this study to adapt data collection and analysis concurrently, providing deeper insights into the drivers, benefits, and challenges of cloud adoption in healthcare. This approach will enhance our understanding of the barriers and facilitators of cloud adoption, informing researchers and healthcare providers.

3.3. Cloud Computing Implementation in Healthcare: Strategies and Challenges

As cloud computing (CC) becomes a leading innovative application and database hosting platform, its adoption in healthcare has been extensively studied. This body of research primarily examines CC's characteristics, features, benefits, and the privacy and security challenges associated with its implementation in healthcare.

The digitization of healthcare organizations and the enhancement of patient record sharing and interoperability through EHR are pivotal in rapidly adopting technologies like CC. The United States projects a compound annual growth rate (CAGR) of 11.58% for EHR CC from 2022 to 2027, reflecting a significant shift in healthcare data creation, processing, sharing, storage, and usage [28]. This growth includes cloud-based services such as telehealth, which healthcare organizations are increasingly adopting to provide clinical services via internet-connected applications. Reference [29] reports that 85% of surveyed physicians use telemedicine, with a majority expressing a continued commitment to this modality for various healthcare services.

Advancements in information technology, notably CC, have revolutionized patient care delivery. CC's ability to provide accessible, reliable, and cost-effective patient data storage has been particularly transformative [30]. However, the ubiquity and convenience of cloud-based data storage also introduce significant security challenges, including concerns about data backup, confidentiality, integrity, and reliability [30].

EHRs, crucial for monitoring health situations, cannot rely solely on Wireless Body Area Networks (WBANs) [31]. Reference [31] emphasizes that integrating Internet of Things (IoT) technologies with CC can significantly enhance the efficiency of the healthcare system. Despite these advancements, concerns about data privacy and security in cloud-based healthcare systems persist.

Akinsanya et al. [32] assessed cybersecurity maturity models in healthcare organizations utilizing CC solutions. They highlight the importance of adhering to security standards and best practices, such as those outlined by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). In addition, HIPAA is crucial for managing healthcare information security within CC architectures [32].

Abrar et al. [9] explore the risks and benefits of CC adoption in healthcare, noting its potential as a scalable and cost-effective solution for security vulnerabilities. However, they also acknowledge the challenges, particularly in cloud service security and resource isolation.

Bamiah et al. [33] assert that CC adoption in healthcare minimizes complexity and enhances EHR management. Nevertheless, the healthcare sector's sensitivity to data breaches due to the nature of the information processed makes it a prime target for cyberattacks [34]. Research from the University of Minnesota's Public Health Department highlights a rise in cyberattacks against healthcare providers from 2016 to 2021, endangering the private health data of over 42 million patients [35]. Disruptions in healthcare organizations frequently manifest as electronic system breakdowns (41.7%), cancellations of scheduled services (10%), and ambulance diversions (4.3%) [35]. In the U.S., where the healthcare sector is a part of critical infrastructure, such disruptions can severely impact patient care and public health. The benefits of using cloud computing (CC) in healthcare are numerous, yet there exists a significant risk of patient harm should sensitive information be compromised [36].

Patient participation is crucial in adopting cloud-based solutions within healthcare, as patient data is collected, generated, processed, and stored in healthcare information management systems [36]. Concerns primarily revolve around unauthorized access or disclosure of patient information due to misconfigured cloud-based solutions [36]. Reference [36] emphasizes maintaining confidentiality, integrity, and availability of patient data in decision-making for cloud-based solutions. They also advocate for ensuring information privacy and security by adopting new technologies like CC in healthcare. Ensuring patient data's confidentiality, integrity, and

availability in healthcare through cloud-based solutions requires robust, security-focused architecture compliant with regulations such as HIPAA.

Healthcare organizations must conduct thorough data security and privacy requirement analyses before CC adoption to ensure information security and privacy in cloud-based solutions. This includes ensuring HIPAA compliance for all cloud-based services handling patient care data. According to [7], following the National Institute of Standards and Technology (NIST) guidance, HIPAA does not mandate a specific gold standard certification but requires adherence to a set of security measures. This distinction is more pronounced in federally recognized healthcare providers than in private entities, which may implement varying cybersecurity safeguards.

Healthcare organizations can assess their readiness for CC adoption using tools such as the Cloud Maturity Model (CMM). Carvalho et al. [37] highlight the development of various maturity models over the past 50 years, which differ in their phases, influencing elements, and sectors of intervention. The OPEN ALLIANCE for Cloud Adoption (OACA) presents the Cloud Maturity Model (version 4.0), consisting of five maturity levels, as outlined by [38]. These levels range from CMM 0, indicating no cloud utilization, to CMM 5, representing optimized orchestration technologies for cloud-based solutions.

This study aims to evaluate the maturity level of cloud-based HIMS adoption in the U.S., focusing on privacy and security concerns. It will utilize Grounded Theory and analyze qualitative data from interviews with healthcare professionals and I.T. specialists involved in cloud-based HIMS. The goal is to ascertain the current state of cloud adoption in HIMS, identify privacy and security challenges, and uncover themes and patterns that may guide future improvements in this field.

4. METHODOLOGY

This qualitative research will explore the interplay between organizational processes and personal experiences, with the researcher's immersion in data collection and analysis being crucial for validity. Constructivist researchers, as noted by [39] Crotty 1998 advocated for onsite engagement to gain insights into participants' environments. Such participation enables researchers to draw precise inferences from their findings. The study will involve direct observation and interviews concerning CC services' provisioning, deployment, maintenance, administration, and security practices. The findings will be synthesized into a theory, systematically organized and categorized, alongside the development of CC security best practices derived from CSPs documentation and whitepapers.

4.1.Research Design

The Grounded Theory approach, essential for ensuring validity and reliability in research studies, encompasses a series of steps: identifying a research problem, formulating a research question, data collection, data coding and analysis, and theory development [40]. This study adopts the Grounded Theory methodology, characterized by its coding processes (Open, Focus, Axial, Selective and Theoretical Coding). This approach facilitates the development of themes and categories through constant comparison, guaranteeing reliable data analysis and formulating a robust, persuasive theory. The iterative strategies inherent in Grounded Theory research permit a simultaneous, careful, and bidirectional approach. This flexibility is crucial for identifying emergent trends within the data analysis process. Reference [41] highlights the method's uniqueness in its concurrent data collection and analysis, emphasizing that the research direction continually informs and shapes the data-gathering process, thereby enriching the analysis.

4.2. Sampling Procedures and Participants

This study employs purposive sampling, a non-probability sampling technique particularly suitable for qualitative research. Purposive sampling enables selection of participants whose characteristics align with the study's needs. This approach is instrumental for qualitative researchers, as it facilitates data targeting directly relevant to the research questions, objectives, and aims [42]. Reference [43] discusses the origins of probability theory-based sampling methods, which date back to experiments in 1948 and are predominantly used for studying subsets of populations; these methods, including random sampling, are primarily pertinent to research that intends to generalize findings to larger populations. However, in the context of qualitative research, where the emphasis lies on an in-depth analysis of detailed information, random sampling is less frequently employed due to issues related to scalability [42]. The current study selected a specific group of participants: ten healthcare professionals and I.T. specialists in a Washington, DC Metropolitan Region healthcare organization, all involved with cloud-based HIMS. The selection criteria for these participants were based on their experience and involvement in using and managing cloud-based HIMS. This purposive sampling strategy ensures that the participants provide valuable insights pertinent to the research question, thereby contributing to a more comprehensive understanding of the subject matter [44].

4.3. Research Instruments

Before the commencement of the interview, participants received an informed consent form to confirm their voluntary participation in the research. The primary source of qualitative data is participant interviews, including individual face-to-face and online formats. The study utilizes open-ended, semi-structured interviews, as it aims to gather qualitative insights. These interviews predominantly explore participants' experiences, perceptions, and descriptions relevant to the study's phenomenon.

All interview questions are carefully crafted to align with the research question, ensuring clarity and precision for participant comprehension. Reference [39] advocated for interviews comprising a limited set of open-ended questions in an informal environment to draw out participants' thoughts and emotions. Observations of participants in their natural settings inform the refinement and development of new interview questions based on emerging concepts and processes.

Each interview is scheduled for a standard duration of 30 to 45 minutes. This timeframe serves as a guideline, allowing flexibility for potential extension beyond the specified limit.

5. DATA ANALYSIS

Data collected from participant interviews, including audio recordings and transcripts, is securely stored using a multi-platform approach. This approach encompasses a password-protected USB Flash Drive, Microsoft OneDrive—a cloud-based storage solution—and Amazon Web Services (AWS) Simple Storage Services (S3). AWS S3, known for its durability and availability, encrypts all data at rest, ensuring protection against unauthorized access [45]. AWS S3's compliance programs and auditing capabilities enhance data security [45].

To respect participants' privacy, their names and the name of the healthcare organization remain anonymous throughout the interview and qualitative data analysis processes. This anonymity is

maintained by assigning each participant a chronological identifier, beginning with "Participant 01" and continuing in sequence.

The audio recordings of the interviews are stored in an audio sub-folder within the Research Database folder and on AWS S3 before transcription. This ensures data durability, redundancy, availability, and security. The audio recordings are transcribed using Amazon Transcribe, an automatic speech recognition service that accurately converts audio into high-quality text [46]. Amazon Transcribe, ensuring secure data transport, employs TLS (Transport Layer Security) 1.2 and AWS certificates for data encryption in transit. It is ideal for applications requiring secure and accurate text representation of spoken content [46].

Upon transcription, the audio-recorded interviews are carefully reviewed for completeness and accuracy compared to the original recordings. Non-codable verbal fillers such as "uh," "ha," and "okay" are carefully omitted without altering the participants' intended messages. Participants are then provided with a copy of their transcripts to review and confirm the accuracy of their responses. Following their confirmation within 24 hours, the final transcripts are stored in specific sub-folders within the Research Database folder on Microsoft OneDrive, categorized by the research question (RQ1). The naming convention for these transcripts combines the participant's identifier, the research question (abbreviated as "RQ1"), and the word transcript (e.g., Participant 01 transcript is "P01-RQ1-transcript").

For qualitative data analysis, the study employs MAXQDA, a robust software for Coding and Analysis. The organized interview data files are imported into MAXQDA's Document System, specifically into a folder named "Interview Transcripts." Before Coding and Analysis, the initial step involves familiarizing oneself with the data, a process facilitated by MAXQDA's memo function.

5.1. Analysing Data and Documenting Observations in MAXQDA: A Methodological Approach

The initial phase of this research involved an in-depth familiarization with the data, a crucial precursor to Coding and Analysis. This study employs the grounded theory methodology, wherein coding and data analysis commences following each participant interview. This process includes conducting, audio-recording, transcribing, validating through member checking, and integrating the interviews into MAXQDA software. An examination of the data before coding and analysis, mainly through transcript review, yielded several vital insights, documented in MAXQDA's free memo feature as listed below:

Transition to Cloud-Based Solutions: The organization is transitioning towards a cloud-based solution for managing Protected Health Information (PHI). Despite this shift, they continue to rely on a trial-and-error approach to identify the most suitable solution.

Challenges in Cloud-Based PHI Management: Implementing cloud-based solutions for PHI management in healthcare encounters numerous challenges, particularly concerning security, compliance, and user experience. Key issues include:

- **Data Confidentiality:** Digitizing and securely storing paper-based patient documentation in cloud-based systems poses significant challenges in maintaining data confidentiality.
- **Learning Curve and User Adaptability**: The introduction of a cloud-based HIMS presents a steep learning curve, primarily due to the non-technical backgrounds of most

staff members. This highlights a disconnect between technological advancements and user adaptability.

Technological Versus Human Factors: A recurrent theme in technology implementation, evident in this case, is the interplay between the efficiency of technological solutions and the challenges associated with user adoption.

Cloud Maturity Model - Opportunistic Stage: The organization currently resides at the "Opportunistic" stage of the Cloud Maturity Model (CMM). This stage is characterized by a purposeful use of cloud services beyond experimentation to address specific problems or seize particular opportunities [38]. At this juncture, cloud technologies are employed more intentionally compared to the ad-hoc, experimental phase but have not yet evolved into a standardized or strategic element of the organization's I.T. infrastructure [38].

Perceived Benefits of Cloud-Based Systems: Participants express a positive outlook on the adoption of cloud-based systems for PHI, particularly noting the enhanced security features such as multifactor authentication, risk analysis for unusual login activities, continuous auditing and reporting, and end-to-end encryption of data at rest and in transit. This perspective emphasizes the security and privacy benefits inherent in cloud-based systems, which are expected to augment patient care delivery and trust.

5.2. Phase of Initial Coding: Systematic Analysis in Grounded Theory Methodology

The first step in the research coding phase involved completing an initial coding process of the interview transcripts. This phase entailed preliminary identifying patterns within the data and the creation of an initial set of codes derived from the transcribed data. The research employed Open Coding, a MAXQDA coding function, as a fundamental component of the Grounded Theory methodology. Open Coding, a data-driven coding procedure, was pivotal in identifying codes during the initial phase. Its significance lies in discovering concepts and categories directly from the data, thereby minimizing researcher bias and establishing a robust foundation for the iterative development of a well-grounded theory.

In the context of Grounded Theory, memos play an integral role in the analytical process. Utilizing MAXQDA Memo Manager, the research engaged tools such as Code Memos and Free Memos during the Open Coding process. These memos in MAXQDA are instrumental in Grounded Theory, providing comprehensive documentation of the researchers' reflections, emotional responses, and intuitive considerations [47]. They provide a reflective space for theory generation, ensuring that the Analysis remains firmly anchored in the data.

After coding the interview transcripts, a critical review and recoding of the codes were conducted. This step was essential to ascertain a definitive relationship between the codes and the data segments. Reviewing and recoding data segments following the initial coding phase is vital in qualitative research methodologies, including Grounded Theory. This process is not merely a procedural step in qualitative Analysis; it is crucial for deepening understanding, ensuring consistency, achieving theoretical saturation, and enhancing the overall quality and credibility of the research findings.

5.3. Phase Two of the Analysis: Systematic Categorization of Initial Codes in Grounded Theory Research

An in-depth examination of the initial codes was undertaken in the research's second phase of the grounded theory data analysis process. This step was pivotal in identifying recurring patterns and themes within these codes, thereby facilitating the formation of categories. Therefore, the name Focused coding. Focused coding requires careful consideration in selecting the initial codes that most effectively and comprehensively categorize the data for insightful analysis [27]. During this categorization phase, several critical measures were conscientiously applied by the researcher:

1. Identifying recurrent ideas and concepts bearing similarities were prioritized, as these suggest emergent themes.
2. Ensure the selection of categories was carefully aligned with the research question guiding the study, ensuring relevance and focus.
3. The distinctiveness of each category was ensured, allowing it to represent specific aspects of the data independently.
4. A careful balance was sought in the breadth and depth of categories, avoiding extremes of being overly broad or excessively narrow to encompass the variation of the selected codes meaningfully.
5. The frequency of codes was closely monitored, with higher frequencies indicating the significance of a category in the thematic landscape of the study.
6. Consistent with the principles of Grounded Theory—the methodology underpinning this research—categories were strategically chosen to contribute constructively towards the emergent theory derived from the data.

Categories were carefully constructed based on the initial codes pertinent to each research question. These selected categories provide a structured and coherent framework for analyzing the codes directly relevant to the research inquiries. They play a crucial role in guiding the development of a Grounded Theory, illuminating patterns and themes that naturally emerge from the data.

Before creating these categories, an extensive process of merging, renaming, and redefining the scopes of codes was undertaken. This process was informed by a deeper, more refined understanding of the transcribed data, thereby enhancing the precision and clarity of the subsequent analytical stages.

In this study, MAXQDA's Code category function systematically organizes categories and codes within the code system. Table 1 showcases these categories and codes pertinent to the selected research question, depicting the rationale behind their selection. After a thorough review and integration process, the initial codes related to the research question are classified into broader themes. These themes emerge from the intrinsic characteristics of the codes and their pertinence to the overarching research question.

Table 1. Categories, Codes, and Rationale for Selection

Category	Codes	Reason for Selection
Cloud Benefits	Improving patient Care Delivery, Improved Efficiency, and Perceived Cloud Adoption Benefits	Codes highlight the positive impacts and advantages of adopting cloud-based systems in healthcare. Grounded Theory methodology involves looking for emerging patterns that can form a theory, and these benefits are significant for theory building.
Security Measures	Data Transmission Integrity, Security Reinforcement, Data Security Improvement, Multifactor Authentication, Risk Analysis, Continuous Monitoring and Alerts, Trust in Cloud Systems and Security, Access Control Management, Data Sensitivity and Handling, Security Investment Priority	Codes emphasize the various security protocols and measures implemented in cloud-based HIMS. The codes share the theme of specific actions to secure patient data in the cloud-based system.
Compliance and Regulation	Financial and Compliance Adherence, HIPAA and HITECH Compliance, Built-in Compliance in Cloud Systems, Compliance Motivation, Service Level Agreement (SLA) Compliance, Policy Oversight	These codes focus on the regulatory and compliance aspects of cloud-based HIMS, ensuring patient data is handled appropriately. The codes share specific compliance features and actions to secure patient data. Codes also directly address the research question's focus on privacy and security improvements through regulatory adherence.
Training and Development	I.T. Intervention, Training and Skill Development, Adaptability, and Learning	These codes stress the importance of training and continuous learning for the staff to use and manage cloud-based HIMS effectively. The codes are distinct from direct security measures, focusing on human factors and learning.
Challenges and Risks	Data Breach Risk, Cloud Adoption Challenges, Insecure Data Transfers, Non-Technical Workforce, User Access Issues	Codes highlight potential challenges and risks the healthcare organization faces with cloud-based adoption.

5.3.1. Comparative Analysis using the MAXQDA Code Relations Browser in Grounded Theory

The initial phase of category creation, essential for structuring the dataset, has successfully laid the groundwork for an in-depth exploration of the research question. This foundational step is imperative for conducting a comprehensive comparative analysis of the identified categories and their subcodes. Utilizing the MAXQDA Code Relations Browser tool is particularly noteworthy in this context. This tool, integral to Grounded Theory's comparative analysis methodology,

offers a visual and qualitative approach to examining code relationships. Its application is instrumental in uncovering latent patterns and connections within the data, enriching our understanding and facilitating a more profound and grounded analysis.

Employing the MAXQDA Code Relations Browser, we visually depict the interrelationships among codes, drawing on qualitative data from interview transcripts. In this visualization, each square symbolizes a coded data segment. The placement of these squares indicates the frequency of coding concerning other codes, offering insightful perspectives on data interconnectivity. This approach enhances the clarity of our analysis and contributes to a more nuanced understanding of the data's underlying structures.

The research question explores the impact of cloud-based computing within HIMS on the protection and confidentiality of patients' PHI in the U.S. Figure 1, featuring the Code Relations Browser from MAXQDA, offers an organized depiction of thematic elements addressing cloud computing's influence on PHI security and privacy in U.S. HIMS.

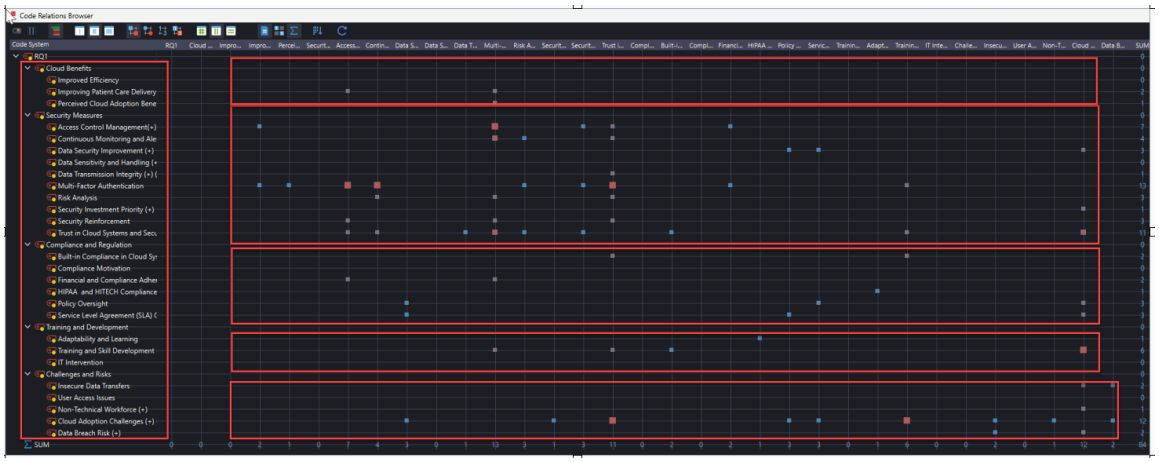

Figure 1. MAXQDA Code Relations Browser

The key themes identified are:

1. **Cloud Benefits**: This theme emphasizes the positive outcomes of cloud computing, notably its role in enhancing efficiency and patient care, which are believed to contribute to PHI's improved management and security.
2. **Security Measures:** This category encompasses specific security protocols, such as access control management and multifactor authentication, to strengthen PHI security.
3. **Compliance and Regulation:** This theme emphasizes their essential role in safeguarding PHI by focusing on adherence to legal frameworks, notably HIPAA and HITECH.
4. **Training and Development**: This theme highlights the significance of training and ongoing skill development. It proposes that human factors like expertise and continuous learning are crucial for PHI protection.
5. **Challenges and Risks:** This theme addresses PHI integrity and security risks by identifying potential vulnerabilities and threats, such as data breaches and insecure data transfers.

Analysis of code size and frequency within these themes reveals a hierarchical importance, with "Security Measures" and "Compliance and Regulation" more prominently featured. This indicates a significant focus in the dataset on these aspects, reinforcing their criticality in the research context of PHI privacy and security in cloud-based HIMS.

Furthermore, the dataset illustrates a linkage between "Training and Skill Development" and "Improved Efficiency," suggesting that training healthcare professionals in cloud-based HIMS enhances efficiency and bolsters privacy and security measures.

The interplay among various codes reveals a refined and holistic relationship between the operational advantages of cloud-based HIMS and the criticality of addressing security and privacy concerns. While cloud computing offers numerous benefits for PHI management, it concurrently emphasizes a careful approach to risk management and compliance with regulatory standards. This equilibrium calls for an in-depth discussion on the necessity of robust security measures, compliance adherence, and proactive risk management in cloud computing to protect PHI.

5.4. Phase Three Analysis: Systematic Formulation of a Core Category in Grounded Theory Research

In this coding phase, the entire dataset was reexamined and reorganized, facilitating the identification and development of a core or central category. This central category serves as the foundation for constructing the Grounded Theory. The primary categories and their respective subcategories, which contain coded data from the research study, contribute to a Grounded Theory explaining how privacy and security are achieved and sustained in healthcare organizations utilizing cloud-based HIMS. This phase uses the Selective coding approach.

Selective coding, an integral process within the Grounded Theory methodology, allows for the emergence of theory directly from the data, abolishing the need for preconceived hypotheses. It involves identifying and systematically interconnecting a central category with other established categories to develop a Grounded Theory [48]. Grounded Theory aims to develop theories firmly rooted in systematically collected and analyzed data. This method involves carefully refining and organizing data, concentrating on isolating a principal category or a central theme that encapsulates the fundamental essence of the research [49]. The appropriateness of selective coding as the pivotal coding process in this research stems from its ability to refine a cohesive, unified theory from the detailed qualitative data. Selective coding aims to foster a comprehensive understanding of the data, culminating in a theory or explanation that fully embraces the observed phenomena [49].

This approach ensured that the research yielded in-depth, actionable insights into the privacy and security aspects of cloud-based HIMS. The selective core or central code, derived from the data, exhibited interrelationships with the main categories and subcategories, thus reinforcing the interconnectedness of the various elements within the study.

Based on the Analysis of the main categories and subcategories derived from participants' data, the core category that emerges for this research study is **Holistic Security, Privacy, and Resilience in Cloud-Based HIMS** (shown in Figure 2 – MAXQDA Code System Hierarchy) around which all the other categories (main and subcategories) and codes are integrated to form a theoretical framework.

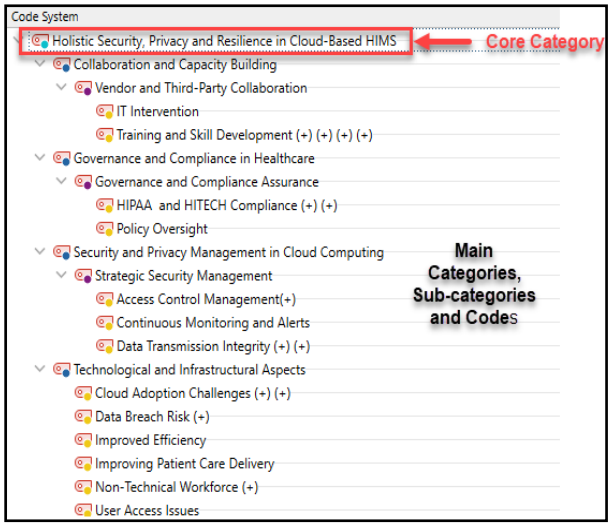

Figure 2. MAXQDA Code System Hierarchy

As it relates to this research study and the analysed data, the core category can further be interpreted as:

1. **Holistic Approach:** The term holistic implies that the security, privacy, and resilience of HIMS in a cloud-based environment are not viewed in isolation. Instead, they are part of an interconnected system that includes technical, human, organizational, and compliance aspects. This approach recognizes that ensuring the security and privacy of HIMS requires a comprehensive strategy that addresses all potential vulnerabilities and involves the entire organization.
2. **Security:** Within the core category, security would encompass the protective measures and protocols to safeguard data from unauthorized access, data breaches, and other cyber threats. This includes cybersecurity protocols, data encryption practices, and access control management. The aim is to protect both the integrity and availability of healthcare data.
3. **Privacy:** Privacy concerns the rights and expectations of individuals regarding their personal health information. This involves ensuring that data is used in accordance with patient consent and compliance with legal frameworks such as HIPAA and HITECH. It also means giving patients control over their information and being transparent about data practices.
4. **Resilience**: Resilience refers to the ability of the HIMS to withstand and recover from incidents that could compromise security and privacy. This could involve incident response strategies, data loss prevention, and disaster recovery plans. Resilient systems are designed to continue operating effectively despite challenges or restore services quickly after a disruption.

Cloud-Based HIMS Considerations:

- **Infrastructure Security:** With cloud-based systems, there is a reliance on the security of the cloud infrastructure itself, including data centers and networks.
- **Vendor Management:** Security and privacy also depend on the relationships with third-party vendors who provide cloud services, necessitating thorough vetting processes and continuous monitoring.

- **Data Governance:** Clear policies regarding data retention, transmission, and deletion are necessary to manage the cloud's lifecycle of sensitive health information.
- **Legal and Regulatory Compliance:** Adherence to relevant laws and industry standards is crucial for legal compliance and maintaining public trust.
- **Education and Awareness:** Training for non-technical staff and ongoing awareness programs are essential to ensure all users understand their role in maintaining security and privacy.

The core category was used to set forth how various factors interact to affect the security, privacy, and resilience of cloud-based HIMS, and it would guide the development of a theoretical framework that aims to improve these systems. As a central theme, the core category is linked to the categories, subcategories, and codes in the participants' provided data, illustrating the interconnectedness and intricacies of maintaining holistic security and privacy in cloud-based healthcare environments.

5.4.1. Utilizing MAXQDA Code Matrix Browser in Grounded Theory Research: A Comparative Analysis Approach

In Grounded Theory methodology, comparative Analysis is a cornerstone process. This procedure stresses the ongoing comparison of data with emerging categories and concepts. The MAXQDA Code Matrix Browser is invaluable during this critical research phase. Its utility facilitates the discernment of themes and patterns, thus enabling a rigorous comparative analysis, a hallmark of Grounded Theory. This approach requires the detailed comparison of each data element with others across the data segments. Engaging in this process is pivotal for refining and explaining the categories that surface from the data.

Figure 3 illustrates the application of the MAXQDA Code Matrix Browser in the current study. This tool provides a systematic framework for analyzing qualitative data, highlighting themes and patterns essential in understanding the impact of cloud-based computing on the privacy and security of PHI in the United States. Within the matrix, each code signifies a unique theme or sub-theme. The color-coded squares (red and blue) indicate the prevalence and frequency of these themes across various data points from research participants' interview transcripts.

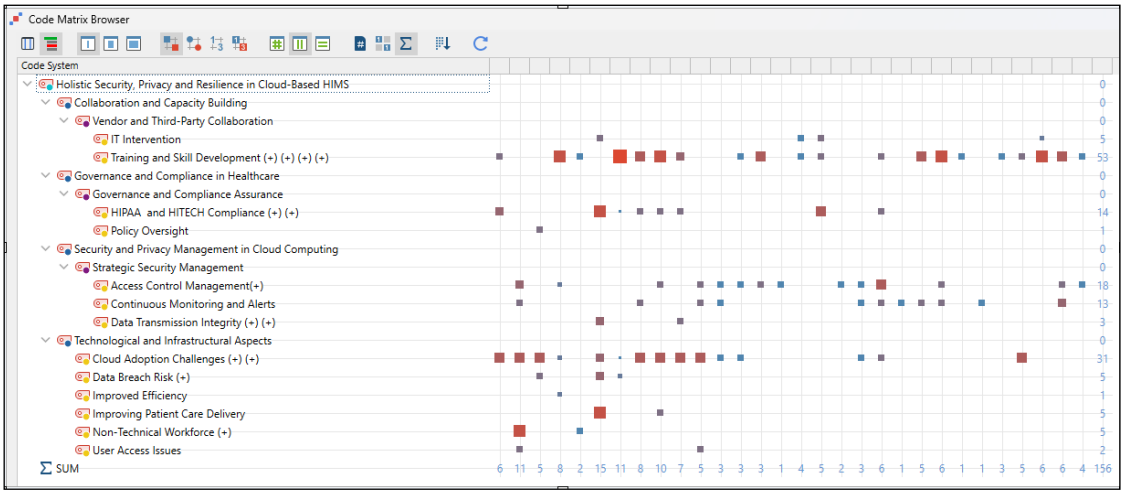

Figure 3. MAXQDA Code Matrix Browser

Specific themes emerge more prominently in the dataset. For instance, "Governance and Compliance in Healthcare," with sub-codes like "HIPAA and HITECH Compliance" and "Policy Oversight," appears recurrently. This prevalence emphasizes the importance of regulatory compliance in cloud-based computing within HIMS. It suggests that these systems are carefully crafted and implemented, prioritizing adherence to legal standards for safeguarding PHI.

Another notable theme is "Strategic Security Management," encompassing sub-codes such as "Access Control Management" and "Continuous Monitoring and Alerts." This theme highlights a proactive stance towards security measures within cloud-based HIMS. Its widespread presence across multiple data points suggests that cloud-based computing enhances PHI security by enabling healthcare providers to manage data access more effectively and vigilantly monitor their systems for potential breaches or unauthorized activities.

The "Technological and Infrastructural Aspects" theme, with sub-codes like "Data Breach Risk" and "Improved Efficiency," indicates a dual awareness: the recognition of technological risks alongside an appreciation for the efficiency enhancements brought about by cloud-based computing. This duality is significant for privacy and security, as more efficient systems may mitigate errors potentially leading to data breaches.

Moreover, the emergence of "Collaboration and Capacity Building" codes reveals that cloud-based computing fosters enhanced collaboration among various entities, which could lead to more robust practices in securing PHI.

A comprehensive analysis of these themes, derived from patterns observed across the interview transcripts, offers a refined understanding of how cloud-based computing is perceived to impact PHI's privacy and security.

6. CODE THEORY MODEL

The Code Theory Model (Figure 4) developed using MAXQDA MAXMaps presents an intricate schematic representation that encapsulates a range of concepts and interrelationships, offering a comprehensive perspective on the safeguarding and confidentiality of patient PHI within cloud-based HIMS in the U.S. This model is the product of a qualitative investigation employing the Grounded Theory methodology, which is instrumental in discerning recurrent themes and patterns emerging from the empirical data. This approach facilitates a deeper understanding of the varied dynamics in managing and protecting PHI in cloud-based healthcare environments.

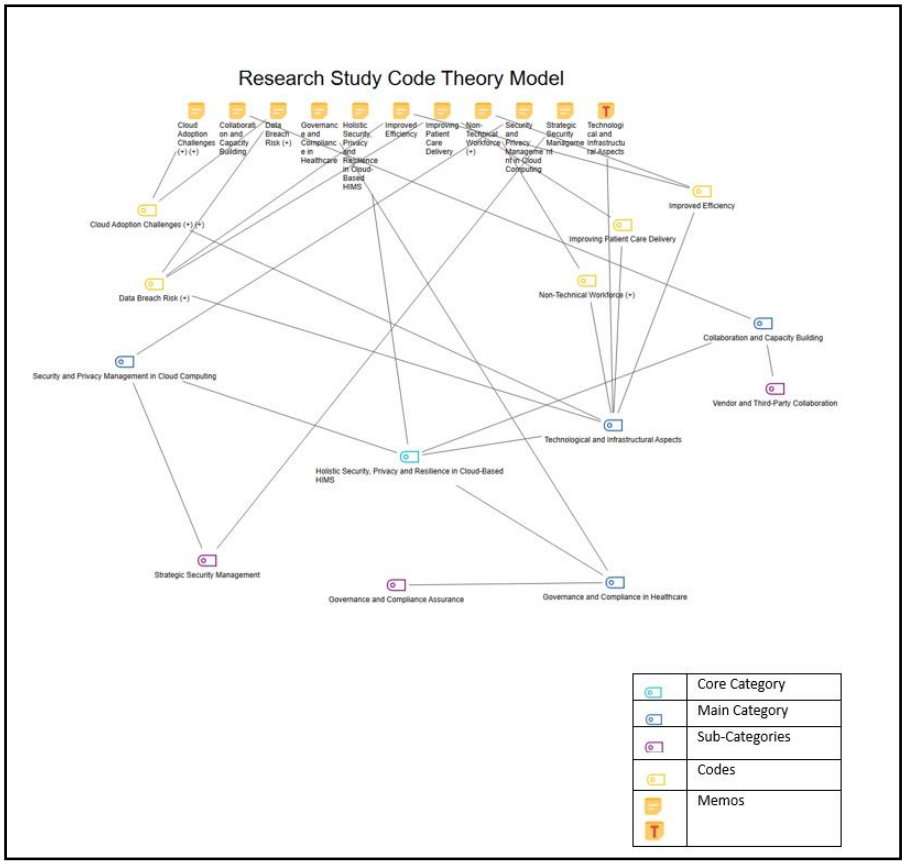

Figure 4. MAXQDA Code Theory Model of Research Study

The framework encompasses a central core category, which acts as the pivotal point of the analysis, integrating and synthesizing the various elements of the data. Surrounding this core are the main categories, which emerge as thematic clusters, encapsulating the prevalent concepts and ideas across the data set. Beneath these main categories lie the subcategories, which serve to further refine and delineate the variances and subtleties within each main category. These subcategories provide a more granular and detailed understanding of the broader themes.

Additionally, the framework incorporates sub-codes, which are even more specific elements derived from the data. These sub-codes enable a deeper dissection of the subcategories, allowing for a more intricate and layered analysis. They are crucial in identifying and highlighting specific instances, patterns, or variations within the data.

Lastly, the framework is enriched with memos and analytical notes compiled throughout the data analysis process. These memos have been critical for capturing reflections, interpretations, and evolving understanding of the data. They serve as a vital tool for documenting the analytical journey, providing a narrative of the coding process, and aiding in developing a cohesive and comprehensive understanding of the research study's findings.

In summary, this intricate framework, derived directly from participant data, offers a holistic and multi-layered perspective essential for thoroughly exploring the research study's focal point: the research question.

6.1. Code Theory Findings

Healthcare organizations in the U.S. have been adopting cloud-based solutions to collect, process, store, and manage patients' health information to improve patient care delivery. In recent years, cloud adoption has become increasingly popular in the healthcare industry to access and store the vast amounts of patient data providers need daily to deliver high-quality patient healthcare services [50]. However, despite the growth in cloud-based healthcare systems, there are still concerns, barriers, and struggles regarding cloud adoption. Some of these barriers are technical, organizational, and human factors limiting the shift to managing patients' PHI in cloud-based HIMS.

6.1.1. Technological and Infrastructural Aspects

Based on the research Code Theory Model, the Technological and Infrastructural Aspects category derived from the participants' data indicates that cloud adoption challenges and risks, especially with the non-technical workforce, can lead to cloud-based systems vulnerabilities and threats. As a result, it poses critical risks to the integrity and security of patient's PHI due to increasing possibilities of data breaches and insecure data transfers. Difficulty in implementing cloud solutions includes both financial constraints and a lack of internal resources. A critical limiting factor in this regard was that organizations lacked the knowledge and abilities to deploy and use cloud capability [22]. As stated by Participant 09 (P09):

> *"First, it took a long time to complete building the cloud system. The time it took was unplanned by the leadership team. The data conversion from paper to digital form contributed to the time as we had boxes of paper health records to convert to digital format. This led to unexpected financial expenses for the organization. The other challenge is getting every staff member up to speed to learn and understand cloud technology." (P09-RQ1-transcript, Pos. 13)*

However, despite the noted challenges and risks, the Technological and Infrastructural Aspects category also indicates significant advantages to adopting cloud-based HIMS to collect, process, and store patients' PHI. Among those advantages identified from the research data, cloud computing adoption in healthcare has streamlined the process of healthcare providers and patients' collaboration, resulting in improved patient care delivery as indicated by Participant 06(P06):

> *"Due to cloud-based EHRs, patient orders can be put in immediately. And wherever the patient might be, it doesn't matter the state or the county; wherever the patient might be can have that lab work done without necessarily coming to the provider's office. It will also automatically be in the system, making it easy for the provider to access the patient's lab report. As a result, this improves patient care delivery by eliminating delays." (P06-RQ1-transcript, Pos. 35)*

Improving the efficiency of patient care delivery from the research data demands implementing strategic security and privacy management policies and procedures across the organization. This brings us to the Security and Privacy Management in the Cloud Computing category achieved from the research data.

6.1.2. Security and Privacy Management in Cloud Computing

The HIPAA Privacy, Security, and Breach Notification Rules (the HIPAA Rules) are essential as they establish crucial safeguards for PHI when created, received, maintained, or transmitted by a HIPAA-covered entity or business associate. These protections include restrictions on the uses and disclosures of PHI, safeguards against unauthorized uses and disclosures, and the rights of individuals concerning their health information [51]. According to the data from the research study, adopting cloud-based HIMS has led to the organization's capability to implement security and privacy safeguards to maintain the confidentiality and integrity of patients' PHI. The strategic security and privacy measures achieved by the healthcare organization's adoption of cloud-based HIMS include:

a) Implementation of Strong Access Control Management Practices and Policies

Robust access control management practices and policies have helped the healthcare organization achieve a cloud security management posture that limits staff access to patients' PHI only on a need-to-know basis. As stated by Participant 10 (P10):

> *"As I mentioned, the cloud has security features for continuous monitoring and auditing that have helped us audit all patient data access logs. The identity access manager also centralizes employees' access and enables the organization to assign roles as the means of access for every employee. This means employees can only access the patient data; they are assigned to access on a need-to-know basis. It is a role-based access control mechanism with strong access controls (P10-RQ2-transcript, Pos. 5)."*

Implementing robust and solid access control management practices to prevent unauthorized access and alteration of patients' PHI on cloud-based HIMS is the responsibility of the customer based on the cloud computing shared responsibility model. It's essential to recognize that the success of security measures in a cloud setting hinges on clearly understanding the boundary between the CSP responsibilities and those of the Cloud Customer. This clarity is crucial in establishing the limitations within a shared responsibility model [52]. Healthcare organizations should understand a robust and secure access control scheme in healthcare cloud computing effectively addresses single-point performance bottlenecks. This approach successfully resolves most security access control challenges [53]. Access management practices can be more effective when backed with continuous monitoring and real-time alerts to log and report all abnormal user behavior activities, such as the unauthorized access, exposure, and dissemination of Patients' PHI.

b) Continuous Monitoring and Alerts

The research study's participants noted that implementing cloud-based systems has equipped the organization to monitor every user activity on patients' PHI in real-time and receive immediate notifications. As indicated by Participant 09 (P09), this is a security strategy that is helping the organization minimize cybersecurity threats against patients' PHI in the cloud-based systems:

> *"We can only measure the effectiveness based on how we will respond to a threat. For now, we use access control mechanisms, auditing, monitoring, and real-time alerts to help minimize all the cybersecurity threats." (P09-RQ3-transcript, Pos. 9)*

This implementation meets the *NIST Special Publication 800-137* requirement, which states that the constant monitoring of threats, vulnerabilities, and the efficacy of security controls furnishes situational awareness that enables risk-informed endorsement of ongoing authorization determinations [54].

The continuous monitoring of user activities backed by providing real-time alerts to designated teams within the organization for a prompt response to minimize insider threats is helping the organization achieve its regulatory requirement's goal of ensuring patient PHI security and privacy. As stated by Participant 10 (P10):

> *"This makes it easy for us to meet all the regulatory compliance requirements, such as patient data confidentiality and integrity, as we can now audit and monitor all the patient data access from a single pane of glass. It always gives us more security and privacy control at our fingertips and everywhere." (P10-RQ1-transcript, Pos. 5)*

Healthcare organizations must remain compliant with the healthcare regulatory compliance laws and have an established regulatory standard they must follow when collecting, storing, handling, and sharing patients' information. Therefore, it is critical that the healthcare organization and its professionals prioritize these regulatory guidelines and set the required safeguards and guardrails around patient's sensitive data. The Governance and Compliance in Healthcare category that emerged from the research participants' data provides more insight into how the healthcare organization achieved that.

6.1.3. Governance and Compliance in Healthcare

The healthcare sector is among the most heavily regulated fields. As such, healthcare entities must maintain clear governance and compliance within their policies and guidelines. This adherence is crucial to meet the regulatory compliance laws and standards applicable to the healthcare organization and its professionals. Adopting the cloud to host and process patients' data is a shared responsibility between the CSP and the healthcare organization as a business entity. No matter the division of security duties between your company and your cloud provider, adhering to your organization's standards and the mandates of regulatory authorities remains your company's obligation. Hence, having well-defined shared responsibilities enables the healthcare organization to concentrate on its cloud-based HIMS security and privacy strategies without overwhelming its staff with the daily operational tasks that fall under the CSP's scope [52]. This brings us to the research study's derived theme, "Policy Oversight."

a) Policy Oversight

It, therefore, takes the healthcare organization to define policies with the responsibility mandates for the CSP, such as Service Level Agreements (SLA). The SLA document is designed to create a shared comprehension of the services, areas of priority, obligations, and assurances offered by the CSP [55]. It carefully maps out the metrics and duties distributed among the parties engaged in cloud configurations, including the duration for reporting or rectifying system malfunctions [55]. The SLA will be the binding contract of CSP's responsibilities and clearly define the service standards they must meet during the contract terms. This assures the healthcare organization that the CSP provides cloud services that will meet the healthcare regulatory compliance requirements. However, the health care organization will also provide due diligence to ensure the required security and privacy measures are in place, providing adequate security and privacy on patients' PHI. As indicated by participant 03 (P03):

> *"My role or the organization's role now is to ensure that the policies and procedures are in place and that we are monitoring our service level agreements (SLAs) to ensure that they are doing everything they are supposed to do for us. Things like encryption, reporting, role-based access controls, and things like that will enhance the protection of PHIs of our individuals." (P03-RQ1-transcript, Pos. 3)*

For healthcare organizations to achieve and maintain HIPAA compliance, it is a regulatory necessity that both the CSP and the healthcare organization strictly fulfill their individual security and privacy responsibilities. This includes safeguarding sensitive patient PHI from unauthorized disclosure, access, sharing, and use.

b) HITECH and HIPAA Compliance

Reference [56] states that to prevent sensitive patient health information from being disclosed without the patient's knowledge or agreement, national standards must be developed under HIPAA, a federal statute. It is, therefore, critical for the healthcare organization to make the CSP acknowledge that, under HIPAA, a CSP is considered a business associate when a healthcare organization (covered entity) hires it to create, receive, retain, or transmit PHI electronically (for example, to process and store electronic PHI) [51].

The research study gathered insights from participants about the security measures they employ to maintain HIPAA compliance. Table 2 showcases responses from some participants regarding the healthcare organization's security and privacy practices and the use of cloud-based systems to adhere to HIPAA standards.

To summarize participants' responses from Table 2, HIPAA compliance takes more than implementing cloud-based EHR systems, especially when handling patients' PHIs, as there's a risk of mistakenly placing documents in the wrong folder. However, advancements in cloud technology, including Optical Character Recognition (OCR) systems, have improved filing accuracy and reduced such errors. Critical practices in maintaining privacy include ensuring that patient charts are closed when not in use, not sharing passwords, and using additional verification methods like patient photos in cloud-based HIMS. Government regulations primarily drive the adoption of cloud-based electronic health record systems. This shift has benefited healthcare organizations and patients by eliminating the need for time-consuming paper documentation. Cloud-based HIMS solutions have enhanced HIPAA compliance through features like role-based access control, multifactor authentication, continuous monitoring, and log access auditing.

Finally, the importance of strict adherence to HIPAA guidelines in patient information disclosure has advised healthcare professionals not to share patient information without proper authorization, highlighting the need for explicit consent before releasing any patient details to third parties. This approach ensures the confidentiality and privacy of patient data within the organization.

Integrating organizational cyber-hygiene practices with PHI data security and privacy protocols in cloud computing derived from the data is crucial for developing an effective Healthcare Compliance Program. However, the healthcare organization must establish a comprehensive compliance plan and program to ensure these practices and cloud-based applications meet HIPAA regulatory compliance standards. This leads us to the research study’s Collaboration and Capacity Building Category, informed by participants’ data.

Table 2: Participants' Interview Responses: Healthcare Governance & Compliance

Participants	Data/Code Location on Interview Transcript	Coded Data (Participants Interview Responses)
Participant 01	P01-RQ1-transcript, Pos. 19	*"I wouldn't say necessarily so because it's easy for you to violate HIPPA, especially if you're scanning and putting the document in the wrong EHR folder. But as time passed, with the cloud, we could develop programs that would read the documents. OCR systems would read the documents and say, this is not the right name that's going to this right folder."*
Participant 06	P06-RQ1-transcript, Pos. 23	*"We ensure that when a chart is open, or a patient chart is open, you don't leave it open. When you're going somewhere, you get off the computer or your desk, make sure it's closed. You don't share your password with anybody. Most of the time, some of the EHRs, aside from the patient data, add extra measures like the patient picture when you open your chart. So that you know, this is exactly the patient I'm working on."*
Participant 08	P08-RQ1-transcript, Pos. 7	*"It is primarily due to a government regulation demanding all healthcare organizations adopt an electronic health record system to manage patient data. The organization decided to take the cloud-based route, which has benefited the organization and its patients. Now, we do not have to complete paper documentation, which was a huge waste of time for the organization and the patient."*
Participant 09	P09-RQ1-transcript, Pos. 11	*"So, as I indicated earlier, you know, the control access to patient data based on roles with multifactor authentication due to the cloud solution has been great in ensuring the organization's compliance with HIPAA. Patient data is also now very organized with the cloud. No more paper documentation of patient records that everyone can pick up easily, regardless of their roles or responsibilities within the organization."*
Participant 10	P10-RQ1-transcript, Pos. 9	*"HIPAA compliance is critical to the organization. The cloud is helping us meet those compliance standards due to its built-in features, such as continuous monitoring and log access auditing."*

6.1.4. Collaboration and Capacity Building

The comprehensive compliance plan across the organization has facilitated effective collaboration in the healthcare organization by enhancing skills. This has led to the development of healthcare professionals' abilities to secure and maintain the privacy of patients' PHI within cloud-based HIMS. From the participants' data, the organization's Training and Skill development program in HIPAA-required policies and security awareness practices has significantly complied with the HIPAA privacy and security rules, which ultimately translates into minimizing and mitigating the likelihood of patient data breaches through HIPAA violations. Training on HIPAA should go beyond merely fulfilling compliance requirements. Educating staff about HIPAA policies and security awareness enables them to carry out their duties compliantly and prevent errors that might lead to privacy breaches. A crucial objective of such training is to safeguard the confidentiality of protected health information and avert any violations of HIPAA regulations [57]. The organization's mandatory requirements for healthcare professionals to

complete the Training and Skill Development programs have positively impacted the security and privacy of patients' PHI in cloud-based HIMS.

From participants' data, Table 3 highlights some participants' responses to the healthcare organization's Training and Skill Development program.

The significance of training and skill development in the context of healthcare data security and privacy is evident from the practices of the organization described by participants. Key strategies derived from the responses (Table 3) that the healthcare organization is implementing to promote the security of privacy of patients' PHI in cloud-based HIMS include:

- **Selection of Superusers:** The organization identified 'superusers' from each department who received specialized training. These individuals played a crucial role in providing support and weekly training to other staff members, ensuring that everyone was competent in securely accessing and using patient data.
- **Multifactor Authentication and Staff Training:** The organization implemented multifactor authentication for data access to protect Patient Health Information (PHI). This technical measure was complemented by extensive staff training, emphasizing the importance of security and reinforcing best practices.
- **Role-Based Access Control:** The I.T. team educated staff on the importance of secure patient data handling. Access to patient information was strictly regulated, with different levels of data visibility assigned based on job roles, ensuring that only authorized personnel could access sensitive information.
- **Peer Support During Cloud Implementation:** During the transition to cloud-based systems, superusers, including those with clinical backgrounds, provided essential support to their colleagues, assisting with documentation and workflow processes. This peer-to-peer support system was instrumental in facilitating a smooth transition.
- **Ongoing Training Programs**: The organization mandated regular training sessions for all staff to continuously reinforce their data security knowledge and address potential vulnerabilities. This ongoing education helped maintain a high patient confidentiality standard and compliance with HIPAA regulations.

In summary, participants' responses indicate that the organization's commitment to continuous training and skill development played a pivotal role in enhancing the security and privacy of patient data, particularly in a cloud-based HIMS. This comprehensive training approach ensured compliance with regulatory standards and fostered a culture of security awareness and responsibility among all staff members.

Table 3. Participants' Interview Responses: Collaboration and Capacity Building

Participants	Data/Code Location on Interview Transcript	Coded Data (Participants Interview Responses)
Participant 04	P04-RQ1-transcript, Pos. 13 P04-RQ1-transcript, Pos. 11	*"The organization picked out heads from the superusers from each department. So, those superusers were effectively trained. They ensure that these super users for each department are readily available to answer any questions and do follow-up training each week. This ensures that the staff know how to access and use the data, but more so in a much safer and more secure way."* *"What was done regarding protecting PHI, of course, is utilizing that multifactor approach to log in to access patients' data and staff training, a lot of staff training for the reinforcement of knowledge."*
Participant 07	P07-RQ1-transcript, Pos. 11	*"The I.T. team teaches us to ensure patient data is secure. This is because you cannot log into any Patient chart unless authorized. The organization also ensures that there are things that I cannot see, but when my boss logs in, she can see other things. So, I believe the access control does it all."*
Participant 07	P07-RQ1-transcript, Pos. 21	"*During the cloud implementation process, I was not working as a nurse, and I was working as a super user. I was helping people with the documentation process, like an elbow support. If you need help and are stuck, I'll come and show you the workflow. It was a lot of us, which was very helpful."*

7. CONCLUSION

Based on the code theory model analysis, there is a clear indication that the adoption of cloud-based HIMS by U.S. healthcare organizations will improve the privacy and security of patients' PHI. However, achieving this involves a holistic approach with several factors considered. First, it will start with healthcare organizations able to define their cloud adoption strategy. A detailed cloud adoption strategy will help healthcare organizations develop a cloud roadmap to identify the cloud adoption challenges they may face while implementing cloud technologies. The Cloud Maturity Model (CMM) provides an essential framework that the healthcare organization can utilize to determine the organization's cloud's maturity level.

Healthcare organizations with precise cloud adoption and implementation strategies can define their cloud-based security and privacy posture to protect the confidentiality and integrity of patients' sensitive data, such as PHI. The cloud-based security and privacy posture will involve implementing an organization-wide strong access management practices for all patients' data access, a proactive security strategy of continuously monitoring and reporting any unauthorized access, use, and sharing of patients' data in real-time. When appropriately implemented, these

security and privacy measures will provide healthcare organizations with the regulatory requirements to be HIPAA compliant.

Achieving HIPAA compliance goes beyond implementing security and privacy services. It requires a comprehensive regulatory and compliance plan that promotes security and privacy practices across the healthcare patients' data lifecycle. For healthcare organizations with cloud-based systems, an established collaboration with CSPs is required in the form of an SLA to define the CSPs' cloud services compliance obligations. Healthcare organizations have their cloud-based environment responsibilities, chief among them being continuously training healthcare professionals and continually upskilling them with the required skills to implement a security and privacy management strategy. Such efforts are crucial for maintaining HIPAA compliance and continuously enhancing the protection and confidentiality of patients' PHI in cloud-based HIMS.

8. RECOMMENDATIONS FOR FUTURE RESEARCH

Building upon this research study's foundational data, a key area for extending the study lies in conducting a comparative analysis across different cloud-based deployment models. This extension would involve a detailed comparison of public, private, and hybrid cloud models currently employed in U.S. HIMS to ascertain their relative effectiveness in safeguarding PHI. Such an analysis is pivotal as each model possesses unique architectural and operational characteristics that influence their ability to protect PHI against breaches and unauthorized access. The study can uncover critical insights into which cloud-based approach offers superior privacy and security features by evaluating variables such as data encryption standards, access control mechanisms, compliance with healthcare regulations like HIPAA, and incident response strategies across these models. This comparative analysis will not only enhance understanding of the strengths and weaknesses inherent in each model but also guide healthcare providers in making informed decisions about the most appropriate cloud architecture for their specific needs in managing sensitive patient data.

9. LIMITATIONS OF THE STUDY

Given the complexity and critical nature of the U.S. healthcare system, this research study encountered several significant limitations:

1) Non-Technical Capabilities and Insufficient Cybersecurity Knowledge Among Healthcare Professionals: Primarily focusing on patient care, healthcare professionals often lack extensive knowledge of cloud-based systems' technical and cybersecurity aspects. This deficiency in technical expertise constrains the depth and accuracy of the information they can offer about the effectiveness of these systems in safeguarding PHI. Furthermore, it resulted in an incomplete understanding of these systems' privacy and security features and the associated potential risks.

2) Sensitivity of Healthcare Data: The highly sensitive nature of healthcare data imposed restrictions on how much information healthcare professionals could disclose. This confidentiality concern limited the researcher's access to in-depth case studies or specific data points concerning implementing and operating cloud-based HIMS. Consequently, these professionals had a notable hesitancy to share insights about their systems, especially regarding vulnerabilities or previous security breaches.

3) Busy Schedules of Healthcare Professionals: The demanding schedules of healthcare professionals posed significant challenges in securing interviews or in-depth discussions. This hindered primary data collection, which is pivotal for a Grounded Theory approach. The limited availability of professionals led to a smaller sample size, potentially affecting the comprehensiveness and representativeness of the study's findings.

These limitations reinforce the need for careful planning in conducting the research effectively. Potential strategies for future research may include leveraging secondary data sources, utilizing anonymized case studies, conducting group interviews or surveys for more efficient engagement with professionals, and focusing the research on specific types of healthcare institutions better to manage the complexities inherent in the U.S. healthcare system.

REFERENCES

[1] Gartner, "Gartner Says More Than Half of Enterprise I.T. Spending in Key Market Segments Will Shift to the Cloud by 2025," Gartner, 2022. https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending

[2] "Healthcare Cloud Infrastructure Market Size, Share 2023-2032," www.precedenceresearch.com, Jan. 2022. https://www.precedenceresearch.com/healthcare-cloud-infrastructure-market/amp (accessed Dec. 21, 2023).

[3] S.-C. Chang, M.-T. Lu, T.-H. Pan, and C.-S. Chen, "Evaluating the E-Health Cloud Computing Systems Adoption in Taiwan's Healthcare Industry," Life, vol. 11, no. 4, p. 310, Apr. 2021, doi: https://doi.org/10.3390/life11040310.

[4] O. Ali, A. Shrestha, J. Soar, and S. F. Wamba, "Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review," International Journal of Information Management, vol. 43, pp. 146–158, Dec. 2018, doi: https://doi.org/10.1016/j.ijinfomgt.2018.07.009.

[5] E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, "Security Challenges in Healthcare Cloud Computing: A Systematic Review," Global Journal of Health Science, vol. 9, no. 3, p. 157, Jul. 2016, doi: https://doi.org/10.5539/gjhs.v9n3p157.

[6] E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, "Security Challenges in Healthcare Cloud Computing: A Systematic Review," Global Journal of Health Science, vol. 9, no. 3, p. 157, Jul. 2016, doi: https://doi.org/10.5539/gjhs.v9n3p157

[7] M. Masrom and A. Rahimli, "Cloud Computing Adoption in the Healthcare Sector: A SWOT Analysis," Asian Social Science, vol. 11, no. 10, Apr. 2015, doi: https://doi.org/10.5539/ass.v11n10p12.

[8] N. Sultan, "Making use of cloud computing for healthcare provision: Opportunities and challenges," International Journal of Information Management, vol. 34, no. 2, pp. 177–184, Apr. 2014, doi: /doi.org/10 https:/.1016/j.ijinfomgt.2013.12.011.

[9] H. Abrar et al., "Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry," IEEE Access, vol. 6, pp. 19140–19150, 2018, doi: https://doi.org/10.1109/access.2018.2805919.

[10] "What is the Cloud Maturity Model and How Does It Improve Cloud Compatibility? | Seagate U.S.," Seagate.com. / https:/www.seagate.com/blog/what-is-a-cloud-maturity-model (accessed Dec. 21, 2023).

[11] "Healthcare Cloud Infrastructure Market Size Report, 2030," www.grandviewresearch.com. https://www.grandviewresearch.com/industry-analysis/healthcare-cloud-infrastructure-market-report#:~:text=It%20is%20anticipated%20to%20boost (accessed Dec. 21, 2023).

[12] H. Journal, "June 2022 Healthcare Data Breach Report," HIPAA Journal, Jul. 20, 2022. https://www.hipaajournal.com/june-2022-healthcare-data-breach-report/

[13] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "eHealth Cloud Security Challenges: A Survey," Journal of Healthcare Engineering, vol. 2019, pp. 1–15, Sep. 2019, doi: https://doi.org/10.1155/2019/7516035.

[14] A. Wolf, "Biggest Healthcare Industry Cyberattacks," Arctic Wolf, Jun. 16, 2021. https://arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/

[15] R. Pradhan, "How enterprises can overcome the growing cloud skills shortage," InfoWorld, Jun. 07, 2022. https://www.infoworld.com/article/3662770/how-enterprises-can-overcome-the-growing-cloud-skills-shortage.html (accessed Dec. 21, 2023).

[16] DivvyCloud , "2020 Cloud Misconfigurations Report," www.govinfosecurity.com. https://www.govinfosecurity.com/whitepapers/2020-cloud-misconfigurations-report-w-6009?highlight=true (accessed Dec. 21, 2023).

[17] Kunle Elebute, "A Grounded Theory of Security and Technical Barriers to the Continuance Use of Cloud Storage by SMEs," Information security and computer fraud, vol. 6, no. 1, pp. 1–7, Dec. 2018, doi: https://doi.org/10.12691/iscf-6-1-1.

[18] R. Mugonza and A. H. Basaza-Ejiri, "Issues Affecting Health Research Collaborations based on Cloud Computing," International Journal of New Technology and Research, vol. 4, no. 9, Sep. 2018, doi: https://doi.org/10.31871/ijntr.4.9.45.

[19] W. Fernández and H. Lehmann, "Achieving Rigour and Relevance in Information Systems Studies: Using grounded theory to investigate organizational cases," DOAJ (DOAJ: Directory of Open Access Journals), vol. 05, no. 01, Nov. 2005.

[20] O. Al-Hujran, E. M. Al-Lozi, M. M. Al-Debei, and M. Maqableh, "Challenges of Cloud Computing Adoption From the TOE Framework Perspective," International Journal of E-Business Research, vol. 14, no. 3, pp. 77–94, Jul. 2018, doi: https://doi.org/10.4018/ijebr.2018070105.

[21] F. Alharbi, A. Atkins, and C. Stanier, "Understanding the determinants of Cloud Computing adoption in Saudi healthcare organizations," Complex & Intelligent Systems, vol. 2, no. 3, pp. 155–171, Jul. 2016, doi: https://doi.org/10.1007/s40747-016-0021-9.

[22] K. Cresswell, A. Domínguez Hernández, R. Williams, and A. Sheikh, "Cloud technology in healthcare: a qualitative study exploring key challenges and opportunities (Preprint)," JMIR Human Factors, vol. 9, no. 1, Jun. 2021, doi: https://doi.org/10.2196/31246.

[23] I. Lawal and Bagiwa, "Impact of Cloud Adoption on the Performance of Organizations: A Facebook and Linked in Survey-Based Analysis," International Journal of Computer Networks and Communications Security, vol. 4, no. 3, pp. 63–77, 2016, Available: https://www.ijcncs.org/published/volume4/issue3/p2_4-3.pdf

[24] V. Salib, "Digital Health Tools Are Perceived as an Advantage to 93% of Physicians," Sep. 2022. Accessed: Dec. 21, 2023. [Online]. Available: https://pharmanewsintel.com/news/digital-health-tools-are-perceived-as-an-advantage-to-93-of-physicians

[25] F. Sadoughi, O. Ali, and L. Erfannia, "Evaluating the factors that influence cloud technology adoption—comparative case analysis of health and non-health sectors: A systematic review," Health Informatics Journal, vol. 26(2), p. 146045821987934, Oct. 2019, doi: https://doi.org/10.1177/1460458219879340.

[26] "Section III: Regulatory Considerations for Cloud Computing | FINRA.org," www.finra.org, Aug. 2021. https://www.finra.org/rules-guidance/key-topics/fintech/report/cloud-computing/regulatory-considerations

[27] K. Charmaz, Constructing grounded theory. Los Angeles: SAGE, 2006.

[28] "US EHR Cloud Computing Market Size & Share Analysis - Industry Research Report - Growth Trends," www.mordorintelligence.com, 2023. https://www.mordorintelligence.com/industry-reports/united-states-ehr-cloud-computing-market (accessed Dec. 21, 2023).

[29] "2021 Telehealth Survey Report," American Medical Association, 2022. Accessed: Dec. 21, 2023. [Online]. Available: https://www.ama-assn.org/system/files/telehealth-survey-report.pdf

[30] S. Bajrić, " Data Security and Privacy Issues in Healthcare," Scholarly Journal, vol. 42, no. 1, pp. 19–27, Mar. 2020, Accessed: Dec. 21, 2023. [Online]. Available: https://www.proquest.com/docview/2401821583?accountid=27975&parentSessionId=jrKppjtVv1wpvO%2FAylOznfI91GldlIS7wvEpqUwlkYY%3D&sourcetype=Scholarly%20Journals

[31] A. Sajid and H. Abbas, "Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges," Journal of Medical Systems, vol. 40, no. 6, May 2016, doi: https://doi.org/10.1007/s10916-016-0509-2.

[32] O. Akinsanya, M. Papadaki, and L. Sun, "Smart Healthcare and Safety Systems Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?," 2019. Available: https://ceur-ws.org/Vol-2348/paper16.pdf

[33] M. Bamiah, S. Brohi, S. Chuprat, and J. Ab Manan, "A study on significance of adopting cloud computing paradigm in healthcare sector," 2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM), Dec. 2012, doi: https://doi.org/10.1109/iccctam.2012.6488073.

[34] E. Maia et al., “8. Security Challenges for the Critical Infrastructures of the Healthcare Sector,” Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures, 2020, doi: https://doi.org/10.1561/9781680836875.ch8.

[35] A. Fox, “Half of ransomware attacks have disrupted healthcare delivery, JAMA report finds,” Healthcare I.T. News, Jan. 10, 2023. https://www.healthcareitnews.com/news/half-ransomware-attacks-have-disrupted-healthcare-delivery-jama-report-finds#:~:text=From%202016%20to%202021%2C%20the (accessed Dec. 21, 2023).

[36] T. Ermakova, B. Fabian, M. Kornacka, S. Thiebes, and A. Sunyaev, “Security and Privacy Requirements for Cloud Computing in Healthcare,” ACM Transactions on Management Information Systems, vol. 11, no. 2, pp. 1–29, Jul. 2020, doi: https://doi.org/10.1145/3386160.

[37] J. V. Carvalho, Á. Rocha, R. van de Wetering, and A. Abreu, “A Maturity model for hospital information systems,” Journal of Business Research, vol. 94, pp. 388–399, Jan. 2019, doi: https://doi.org/10.1016/j.jbusres.2017.12.012.

[38] B. Wilson et al., “OPEN ALLIANCE FOR CLOUD ADOPTION USAGE MANUAL: CLOUD MATURITY MODEL,” 2018. Accessed: Dec. 21, 2023. [Online]. Available: https://www.oaca-project.org/wp-content/uploads/2018/10/CloudMaturityModelUMv4-0.pdf

[39] J. W. Creswell and J. D. Creswell, Research Design: Qualitative, quantitative, and Mixed Methods Approaches, 5th ed. SAGE Publications, 2018.

[40] V. Bitsch, “Qualitative Research: A Grounded Theory Example and Evaluation Criteria,” Journal of Agribusiness, vol. 23, no. 1, 2005, doi: https://doi.org/10.22004/ag.econ.59612.

[41] K. Charmaz, Constructing Grounded Theory, 2nd ed. London: Sage Publications, 2014.

[42] S. J. Tracy, Qualitative Research Methods : Collecting evidence, Crafting analysis, Communicating Impact, 2nd ed. Hoboken, New Jersey: John Wiley & Sons, Inc, 2020.

[43] E. Babbie, Practice of social research, 15th ed. S.L.: Cengage Learning, 2021.

[44] J. Sargeant, “Qualitative Research Part II: Participants, Analysis, and Quality Assurance,” Journal of Graduate Medical Education, vol. 4, no. 1, pp. 1–3, Mar. 2012, Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3312514/

[45] Amazon Web Services, “What is Amazon S3? - Amazon Simple Storage Service,” docs.aws.amazon.com, 2023. https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html

[46] “What is Amazon Transcribe? - Amazon Transcribe,” docs.aws.amazon.com, 2023. https://docs.aws.amazon.com/transcribe/latest/dg/what-is.html

[47] Y. Chun Tie, M. Birks, and K. Francis, “Grounded theory research: A design framework for novice researchers,” SAGE Open Medicine, vol. 7, no. 1, pp. 1–8, Jan. 2019, doi: https://doi.org/10.1177/2050312118822927.

[48] M. Vollstedt and S. Rezat, “An Introduction to Grounded Theory with a Special Focus on Axial Coding and the Coding Paradigm,” ICME-13 Monographs, pp. 81–100, 2019, doi: https://doi.org/10.1007/978-3-030-15636-7_4.

[49] D. Siegle, “Open, In Vivo, Axial, and Selective Coding | Educational Research Basics by Del Siegle,” Educational Research Basics by Del Siegle - Open, In Vivo, Axial and Selective Coding, Jun. 19, 2023. https://researchbasics.education.uconn.edu/open-in-vivo-axial-and-selective-coding/ (accessed Dec. 21, 2023).

[50] Jacqueline LaPointe, “From Head in the Clouds to On the Ground Cloud-Based Revenue Cycle Management,” RevCycleIntelligence, Sep. 06, 2022. https://revcycleintelligence.com/features/from-head-in-the-clouds-to-on-the-ground-cloud-based-revenue-cycle-management (accessed Dec. 21, 2023).

[51] Office for Civil Rights (OCR), “Guidance on HIPAA & Cloud Computing,” Guidance on HIPAA & Cloud Computing, Oct. 23, 2023. https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html (accessed Dec. 21, 2023).

[52] “Shared Responsibility Model Explained,” Cloud Security Alliance - Shared Responsibility Model Explained, Aug. 26, 2021. https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/ (accessed Dec. 21, 2023).

[53] R. Sivan and Z. A. Zukarnain, “Security and Privacy in Cloud-Based E- Health System,” Symmetry, vol. 13, no. 5, p. 742, May 2021, doi: https://doi.org/10.3390/sym13050742.

[54] K. Dempsey et al., “NIST Special Publication 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” NIST SP 800-137,

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, Sep. 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf (accessed Dec. 21, 2023).

[55] J. Montgomery and S. Lelii, "What is a Cloud SLA (Cloud Service-Level Agreement)?," TechTarget - cloud SLA (cloud service-level agreement), 2023. https://www.techtarget.com/searchstorage/definition/cloud-storage-SLA#:~:text=A%20cloud%20SLA%20(cloud%20service%2Dlevel%20agreement)%20is%20an (accessed Dec. 21, 2023).

[56] CDC, "Health insurance portability and accountability act of 1996 (HIPAA)," Centers for Disease Control and Prevention, Jun. 27, 2022. https://www.cdc.gov/phlp/publications/topic/hipaa.html

[57] Steve Alder, "HIPAA Training Requirements," HIPAA Journal - HIPAA Training Requirements, 2018. https://www.hipaajournal.com/hipaa-training-requirements/ (accessed Dec. 21, 2023).