**Cloud Based Healthcare Management: A Case Study on Enhancing Security through AWS Architecture**

Namrata Mali

malinamratavijay@cityuniversity.edu

Zeinep Zhorobekova

zhorobekovazeinep@cityuniversity.edu

Likhitha Lakshmi Gudivada

gudivadalikhithalak@cityuniversity.edu

Siraphat Mingsorn

mingsornsiraphat@cityuniversity.edu

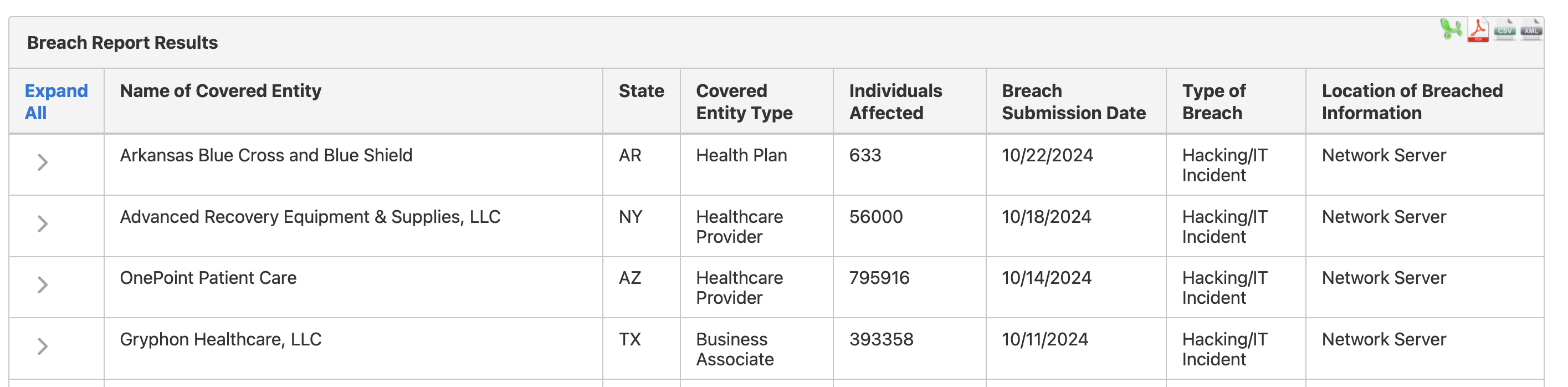
School of Technology & Computing

City University of Seattle

Seattle, WA 98121, USA

**Abstract**

This paper presents a case study examining the potential of deploying a digital healthcare management website utilizing cloud-based architecture to enhance security and operational efficiency considering recent data breaches affecting the U.S. healthcare sector. The U.S. Department of Health has highlighted a significant data breach impacting the sensitive information of approximately 800,000 individuals in a recent case of OnePoint Patient Care data breach incident as shown in Figure 1, which occurred on a network server that lacked the robust security measures available in cloud environments [12]. Given that healthcare is a highly human-centric field, it requires significant human intervention for daily tasks, including patient management, staff scheduling, and safeguarding confidential patient records. By transitioning to a cloud-based infrastructure, healthcare institutions can secure sensitive data, enhance scalability, and improve overall operational efficiency. A well-designed cloud architecture offers a solid foundation that inherently mitigates risks associated with data breaches. This approach not only safeguards patient information but also fosters transparency and effective communication between patients and healthcare providers. Moreover, utilizing a dedicated cloud environment presents a more reliable solution compared to traditional third-party hosting options, where data integrity is often compromised. The proposed cloud architecture not only addresses the immediate concerns of data security but also lays the groundwork for future innovations in healthcare management, including potential integrations with Artificial Intelligence (AI) and Machine Learning (ML) technologies, leading to improved patient outcomes and advancements in healthcare delivery [2].



**Figure 1 [6]**

**Keywords:** Cloud-based Healthcare, Data Security, Digital Health Transformation, Data Breach Prevention

1. **INTRODUCTION**

Recently, there has been a significant change in the healthcare sector towards utilizing cloud-based technology as shown in Figure 2, leading to a push for updating systems to boost efficiency, enhance patient care, and improve data organization [1]. Recent statistics show that around 90% of healthcare organizations are currently using cloud services, with roughly 60% choosing third-party providers to help with the transition [4]. Nevertheless, data breaches continue to happen at alarming rates, even with the extensive use of cloud technologies, often due to insufficient security measures and improper cloud architecture.

In this difficult environment, moving towards a safe cloud framework, especially with the use of AWS, offers a chance for healthcare institutions to tackle these dangers. AWS provides an extensive solution that guarantees top-notch data security and compliance with healthcare regulations while also delivering advanced tools for efficient data management, analytics, and scalability. Healthcare organizations can greatly minimize the dangers of data breaches and gain improved performance and reliability by utilizing AWS's infrastructure.

The main purpose of implementing AWS is to establish a protected cloud setting that alleviates the significant worries about data integrity experienced by healthcare entities, especially smaller firms with limited IT capabilities. By updating their processes with a trustworthy cloud service, these companies can utilize new technologies to improve patient care and efficiency, all while protecting sensitive data.

Most of the participants believe that cloud computing is vital for enabling preventive care, consolidating medical records, and supporting low-income communities. Additionally, a large portion of the population acknowledges the advantages in enabling remote diagnosis and care.

A screenshot of a phone

Description automatically generated

**Figure 2 [5]**

This article will explore how AWS cloud structure can help healthcare institutions address security obstacles and prevent significant data breaches. The discussion will highlight the significance of choosing a strong and safe cloud infrastructure, and show how AWS solutions can boost data protection, streamline workflows, and enhance patient outcomes. By embracing AWS cloud-based healthcare management, companies can prepare for expansion, making sure they address the demands of the digital era and provide top-notch care to patients. This article will investigate how AWS cloud structure can aid healthcare institutions in addressing security obstacles and preventing significant data breaches witnessed as in Figure 3. The conversation will highlight how choosing a strong and safe cloud infrastructure like AWS can boost data protection, simplify processes, and enhance patient results. By embracing AWS cloud-based healthcare management, organizations can prepare for expansion, making sure they address the obstacles of the digital era and provide outstanding care to patients.

1. **BACKGROUND**

The healthcare sector is experiencing a major shift, more and more depending on cloud-based systems to boost efficiency, improve patient treatment, and simplify data handling. With organizations aiming to update their operations, the use of cloud services has increased, with 90% of healthcare organizations reportedly using cloud technology (Cloud Comparison Tool, 2023).   
  
As the healthcare environment changes, it is crucial for organizations to implement strong security measures that are specifically designed for their cloud setups. Studies show that a lot of healthcare facilities are not well-equipped to handle these issues, emphasizing the urgent requirement for thorough plans to reduce risks related to cloud computing (Healthcare Data Breaches, 2023).

A screenshot of a data report

Description automatically generated

**Figure 3**

This article discusses the importance of adopting secure cloud structures, specifically using AWS, to improve data security and adherence to healthcare laws. By tackling the specific security issues linked to cloud-based healthcare management, companies can enhance protection of sensitive patient data and strengthen their operational resilience.

1. **USEFULLNESS**

The shift to cloud-based solutions in healthcare has attracted much interest for its ability to improve operational efficiency, cut costs, and enhance patient care. Many research studies point out the advantages of cloud technology in the field of healthcare, such as enhanced access to data, increased collaboration among healthcare professionals, and more efficient workflows. A study conducted by Raghupathi and Raghupathi (2020) [10] highlights the way cloud computing allows healthcare organizations to handle vast amounts of data efficiently, leading to enhanced decision-making and better patient results.

Additionally, cloud solutions provide healthcare institutions with the ability to adapt quickly to evolving demands, especially during times of public health crises.

Even with these benefits, the growing amount of data breaches in the healthcare industry highlights the urgent requirement for strong security measures [9]. Healthcare organizations face some of the highest rates of data breaches, which showcase the risks linked to poorly configured cloud environments. This has led to an increase in research aimed at creating models and guidelines for securing cloud systems in healthcare environments.

To sum up, despite the various benefits cloud-based solutions offer to healthcare, it is crucial to tackle the security issues that come with them. Continuing studies and the establishment of top practices for cloud structure can greatly enhance data security and safeguarding confidential patient data. Healthcare organizations can improve patient care and operational efficiency by using the knowledge gained from similar projects to help them with adopting cloud technology and noted by the source as per the below figure.

A graph of data on a white background

Description automatically generated

**Figure 4 [8]**

1. **Investing Data Breach Incident**

In July 2024, OnePoint Patient Care (OPPC), a top provider of hospice and palliative pharmaceutical services, experienced a major data breach event [13]. The company's reputation took a big hit due to this event, putting the data of almost 800,000 patients at risk. The leaked data consisted of names, birth dates, SSNs, and medical files. The situation exposed weaknesses in OPPC's current data system, prompting a reevaluation of their cyber defense strategy.

**Analysis of Causes**

A diagram of data breach issues

Description automatically generated

**Figure 5**

Based on the provided materials and additional sources, several key factors contributed to the data breach as per the above figure:

1. **Centralized Data System:** OPPC employed a centralized data architecture where all data was stored in a single repository.

While this approach simplifies management, it creates a "single point of failure." When the central repository is compromised, attackers gain access to the entire dataset. In this case, there were insufficient safeguards like data-at-rest encryption or distributed storage systems.

2. **Outdated Security Infrastructure:** The investigation revealed that OPPC relied on legacy systems lacking regular updates.

These systems were vulnerable to modern cyberattacks due to:

- Weak Encryption: Sensitive data was either poorly encrypted or not encrypted at all.

- Inadequate Threat Monitoring: The breach remained undetected for two days, indicating weaknesses in intrusion detection systems (IDS).

-Poor Access Controls: Role-based access control (RBAC) vulnerabilities allowed unauthorized access.

3. **Lack of Network Segmentation:** Network segmentation isolates parts of a network to limit the spread of an attack. OPPC failed to implement segmentation, enabling attackers to access a larger volume of data after breaching the system.

4. **Third-Party Risks:** OPPC's use of third-party software and services potentially introduced vulnerabilities. Risks included:

- Poor vulnerability management by vendors.

- Insufficient security evaluations of third-party integrations.

A diagram of a tree with a root system

Description automatically generated

**Figure 6**

The data breach incident at OnePoint Patient Care serves as a crucial lesson for the company and the healthcare industry at large.

The key takeaway is the necessity of continuous system updates, improved incident response procedures, and fostering a culture of cybersecurity. Figure 6 highlights the inadequate measures which can be taken care of as initial measures. These measures are essential to ensure patient data protection and system reliability.

1. **OnePoint Patient Care’s Previous Architecture**

The detailed technical architecture of OnePoint Patient Care (OPPC) prior to the breach, as that information has yet to be explicitly detailed in public disclosures. However, based on industry practices and the nature of the breach, some insights can be inferred:

**Centralized Data Systems**

Centralized data systems are architectures where data is stored and managed in a single repository to manage sensitive information efficiently and make it more convenient for management. However, it also introduces risks if the entire system can be affected if the central server or storage is compromised due to cyberattacks, hardware failure, or design flaws.

**Outdated Security Infrastructure**

Outdated security infrastructure is a significant risk for organizations with vulnerabilities that will make the issue happen, such as the systems, software, or hardware that no longer receive updates, patches, or support. The breach's success suggests the presence of outdated or insufficient security measures. In OnePoint Patient Care (OPPC), possibly cause of these details, for example:

1. Weak Encryption: The sensitive information may not have been encrypted both at rest and in transit
2. Limited Threat Detection: The breach went undetected for two days, indicating gaps in real-time monitoring and intrusion detection systems.
3. Poor Access Controls: Unauthorized access implies a lack of strict role-based access control (RBAC) or multifactor authentication (MFA) protocols.

**Legacy Systems**

These systems become a weak link in IT infrastructure, which tells healthcare data to potential risks because healthcare organizations often operate legacy systems that struggle with modern cybersecurity tools. These outdated systems lack the ability to support current security protocols and updates, making them vulnerable to cyber threats.

**Lack of Network Segmentation**

Network segmentation is a critical security practice that isolates different parts of a network to limit the scope of an attack. In cases where data breaches occur, such as the example implied, the exposure of a large dataset often points to insufficient network segmentation. Without this protective measure, attackers can access the entire network once they breach a single system.

**Third-Party Risk**

Organizations like OnePoint Patient Care (OPPC) that rely on third-party software or cloud services are inherently exposed to risks originating from those external vendors, especially if vendor security practices are insufficient. They can become an entry point for attackers, potentially compromising the organization's sensitive data.

Incident Response and Notification Delays

The delay in notifying victims of OnePoint Patient Care's data breach shows significant gaps in their incident response protocols. These delays risk victim protection, fail to meet regulatory requirements, and harm organizational credibility.

1. **AWS HIPAA Program and Shared Responsibility Model**

The Health Insurance Portability and Accountability Act (HIPAA) compliance package on AWS helps healthcare businesses process, store, and transmit protected health information (PHI) in a secure manner. AWS's program is based on the shared responsibility model, which assigns specific roles to the client and AWS to maintain security and compliance [11].

**Shared Responsibility Model for HIPAA Compliance**

AWS’s Responsibilities: The physical infrastructure and core services like computing, storage, and networking are all under the control of AWS, which also manages the security "of" the cloud. In addition to maintaining necessary services like network firewalls and encryption tools, AWS guarantees that data centres correspond to industry requirements for environmental and physical security measures.

Customer Responsibilities: Customers are in responsibility for maintaining security "in" the cloud, which means they must properly handle PHI data, create access controls, and configure AWS services. For example, it is the customer's responsibility to ensure compliance with HIPAA regulations by putting encryption, access control, and appropriate configuration into existence.

**Security Services in AWS’s HIPAA Environment**

AWS provides HIPAA-compliant services, including AWS Lambda for serverless, scalable computing, Amazon S3 for safe data storage, and Amazon RDS for database administration. These systems' integrated compliance capabilities enable businesses to monitor access logs, deploy end-to-end encryption, and identify irregularities instantly.

To assist healthcare businesses in monitoring activity and configuration changes inside their environment, AWS offers solutions such as AWS CloudTrail and AWS Config. By offering data on resource setups, access patterns, and possible security threats, these solutions help to maintain compliance.

**Best Practices for HIPAA Compliance on AWS**

Data Encryption: Use AWS Key Management Service (KMS) or alternative encryption techniques to protect sensitive data while it is in transit and at rest.

Access Control and Monitoring: For role-based access control, make sure that only authorized users have access to PHI by utilizing AWS Identity and Access Management (IAM). Activating multi-factor authentication (MFA) enhances user verification even more.

Audit and Incident Response: AWS offers logging features and audit trails to identify, address, and recover from security events. Having a strong incident response plan in place is essential for dealing with possible breaches or illegal access as soon as possible.

This figure shows how healthcare organizations leveraging AWS services for compliance with HIPAA regulations apply the Shared Responsibility Model. It draws attention to the different roles and responsibilities that AWS and the consumer (a healthcare organization) perform when maintaining data security and privacy.

A diagram of a health care company

Description automatically generated

**Figure 7**

Utilizing AWS's HIPAA compliance program and following the shared responsibility model can help One Point Patient Care build a safe, reliable cloud environment for our project. AWS's integrated compliance tools and strong encryption solutions ensure that companies adhere with legal obligations and reduce security threats, especially those related to data access and breach avoidance. One Point Patient Care can preserve patient confidentiality, assure regulatory compliance, and uphold confidence in their cloud-based infrastructure by conforming to AWS's procedures.

1. **APPROACH**

In this research, we propose a robust cloud architecture tailored specifically for OnePoint Patient Care that prioritizes data security and network integrity. Given the increasing frequency of data breaches and the unique vulnerabilities associated with cloud environments, our approach focuses on implementing a secure architecture that adheres to best practices as shown in the below two figures for safeguarding sensitive patient information.

A diagram of a cloud architecture

Description automatically generated

**Figure 8**

A diagram of a cloud architecture

Description automatically generated

**Figure 9**

By following these guidelines, OnePoint Patient Care can create a robust cloud architecture that not only enhances operational efficiency but also significantly mitigates the risks associated with data breaches, ensuring the confidentiality and integrity of sensitive patient information.

1. **SUGGESTED AWS ARCHITECTURE FOR ONEPOINT PATIENT CARE**

Understanding OnePoint Patient Care's Data Needs and Processes

#### 1. Types of Data Stored:

#### OnePoint Patient Care, as a healthcare business, deals with the following categories of data:

1. Patient Data (Structured):
   1. Patient profiles, prescriptions, and treatment histories.
   2. Demographics, medical records, and billing information.
   3. Compliance mandates, such as HIPAA, require stringent data security and privacy measures.
2. Operational Data (Semi-Structured):
   1. Logs from applications, services, and infrastructure.
   2. Monitoring and telemetry data for business operations.
3. Analytics and Reporting Data (Structured/Unstructured):
   1. Aggregated clinical data for insights into patient outcomes or operational efficiencies.
   2. Reports for regulatory bodies or internal decision-making.
4. Archival Data (Structured and Unstructured):
   1. Long-term storage of historical patient data and audit logs.
   2. Older datasets need to be cost-effectively retained for legal or compliance purposes.

#### 2. How the Data Is Processed:

1. Real-Time Processing:
   1. Processing of incoming data streams, such as new prescriptions, patient orders, and event logs.
   2. Real-time anomaly detection for system security or patient care alerts (e.g., flagging risky drug interactions).
2. Batch Processing:
   1. Periodic updates to patient records and billing systems.
   2. Generating reports for stakeholders or compliance requirements.
3. Data Analytics and Insights:
   1. Using historical and operational data to derive trends or actionable insights (e.g., predicting medication demand or improving patient outcomes).
4. Secure Data Sharing:
   1. Sharing patient data with authorized entities while maintaining compliance with regulations like HIPAA.

For OnePoint Patient Care, a healthcare business dealing with sensitive patient and operational data, the selected AWS architecture ensures secure, efficient, and scalable data management. The company needs a robust solution to handle large volumes of structured, semi-structured, and unstructured data while adhering to strict regulatory compliance, such as HIPAA. Additionally, processing requirements span real-time data streams, batch processing, and analytics. The following AWS services as per below figure have been chosen based on their ability to address these specific data processing needs while ensuring the protection and availability of critical healthcare data.

A diagram of a data storage system

Description automatically generated

**Figure 10**

The AWS services chosen to align with OnePoint Patient Care's data needs and processes, ensuring scalability, security, and efficiency and is summarized in the figure 11:

1. S3: Chosen for storing raw and archival data due to its scalability and cost-effective storage, ideal for patient profiles and historical records.

2. RDS: Selected for transactional data, offering structured data storage and management, suitable for patient records and billing.

3. DynamoDB: Opted for logs and semi-structured data, providing fast access and high availability.

4. Lambda: Supports real-time processing, such as flagging anomalies or processing new prescriptions.

5. EC2: Handles batch processing tasks like updating patient records or generating reports.

6. Athena & Quicksight: Used for querying and analyzing operational data to generate insights, including trend analysis and reporting.

7. IAM & KMS: Ensure HIPAA compliance by managing secure access and encrypting sensitive data.

8. CloudWatch: Provides continuous monitoring of all services for security and operational health.

A diagram of a software company

Description automatically generated with medium confidence

**Figure 11 [3]**

1. **WORKLOAD ASSIGNMENT**

|  |  |
| --- | --- |
| Team Member | Work Assigned |
| Namrata Mali (Lead) | Suggesting AWS architecture, research on OnePoints data process |
| Zeinep Zhorobekova | Invested the data breach incident |
| Likhitha Gudivada | HIPPA and shared responsibility model |
| Siraphat Mingsorn | OnePoints previous architecture research |

1. **REFERENCES**
2. Thomas, M. (2024, July 17). Cloud computing in healthcare: How it is used and 15 examples. *Built In*. <https://builtin.com/articles/cloud-computing-in-healthcare>
3. Amazon Web Services, Inc. (n.d.). *End-to-end data and AI strategy for healthcare and life sciences on AWS* [Video]. Amazon Web Services, Inc. <https://aws.amazon.com/health/>
4. Amazon Web Services, Inc. (n.d.). *Are you well-architected?* [Video]. Amazon Web Services, Inc. <https://aws.amazon.com/architecture/?cards-all.sort-by=item.additionalFields.sortDate&cards-all.sort-order=desc&awsf.content-type=all&awsf.methodology=all&awsf.tech-category=all&awsf.industries=industry%23healthcare&awsf.business-category=all>
5. Healthcare leads in third-party data breaches, says new report. (2024, June 25). *Healthcare IT News.*<https://www.healthcareitnews.com/news/healthcare-leads-third-party-data-breaches-says-new-report>
6. Major health data breaches: How are trends shifting in 2024? (“Major Health Data Breaches: How Are Trends Shifting in 2024?”) (n.d.). *BankInfoSecurity.*<https://www.bankinfosecurity.com/major-health-data-breaches-how-are-trends-shifting-in-2024-a-25749>
7. U.S. Department of Health & Human Services - Office for Civil Rights. (n.d.). *Breach report portal.*<https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=08483003DCC03C736AC6F9B47B953835>
8. Office of the National Coordinator for Health Information Technology (ONC). (2024, October). *Health IT.*<https://www.healthit.gov/>
9. Gartner. (2024). *2024 tech trends in healthcare.* Gartner. <https://www.gartner.com/en/digital-markets/insights/2024-tech-trends-in-healthcare>
10. Verizon Business. (n.d.). *2024 Data Breach Investigations Report.* Verizon Business. <https://www.verizon.com/business/resources/reports/dbir>
11. Google Scholar. (n.d.). *Search for Raghupathi and* *Raghupathi (2020).* <https://scholar.google.com/scholar?q=Raghupathi+and+Raghupathi+2020&hl=en&as_sdt=0&as_vis=1&oi=scholart>
12. Use AWS Artifact to accept agreements for multiple accounts in your ORG. (n.d.). [Video]. Amazon Web Services, Inc. <https://aws.amazon.com/compliance/hipaa-compliance/>
13. Paganini, P. (2024, October 25). OnePoint Patient Care data breach impacted 795916 individuals. Security Affairs. <https://securityaffairs.com/170247/data-breach/onepoint-patient-care-data-breach.html>
14. N2K Networks. (2024, October 25). UnitedHealth breach numbers confirmed. [Video]. YouTube. <https://www.youtube.com/watch?v=mgI1FYedQzA>