Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11 , November - 2025

Initiative to Study and Analyze the Effects of Cyberattacks on Healthcare Facilities

Ali Yaslam Omar Basalama,
Bachelor of Systems Analysis, Solutions By STC, Jeddah Saudi Arabia

The worst part about cyberattacks on medical facilities is that many threat actors are likely very well aware of how their attacks affect the lives of people under the care of the healthcare sector, yet the need to protect human lives is outweighed by the financial gain and other motives. And it is now among the sectors most targeted by cyberattacks globally [2]. Due to its immutability, the information accessed through health data breaches is of particular interest to criminals [3]. Blood type, past surgeries and diagnoses, and other personal health information are contained in an individual's medical file. As these records include private data such as name, date of birth, insurance and health provider information, as well as health and genetic information, it is not possible to restore privacy or to reverse psychosocial harm when private data are compromised. These sorts of attacks are not only a threat to patients' identity and finances, but they can also impede hospital operations and place the health and well-being of patients at risk.

WHY IS HEALTH CARE PRONE TO CYBER-ATTACKS?

The emergence of health care as a preferred target for cyber-attacks is relatively recent. Health care, including hospitals, clinics and health insurance, are increasingly undergoing digital transformation to the benefit of patients and cost-efficiency of their services. This is often happening without enough attention being paid to the new risks this brings to the table. The vast amount of critical digital information held by health services (e.g. within patient monitoring systems/electronic health records), coupled with inadequate security (lack of staff awareness and technical safeguards) makes them a prime target for cyber-criminals. For cyber-criminals, withholding access to these time-sensitive data and systems for a ransom is an easy money-making exercise. Cyber-criminals have recognized and learned to exploit this at scale for financial benefit over the past decade. During the COVID-19 pandemic, many healthcare organizations increased their use of digital systems and rapid access to patient data became critical, prompting cyber-criminals to target healthcare as they thought ransoms were more likely to be paid due to the critical nature of the data and systems they were locking access to.

HOW DOES A CYBER-ATTACK AFFECT PATIENTS?

Cyber-attack can have different effects. Cyber-attack can have a direct impact on patient safety and care delivery in a variety of ways. For example, when a healthcare organization is hit with a cyber-attack, the attackers may gain access to sensitive patient data, including personal information, medical histories and even financial information. In some extreme cases, cyber-attacks have even led to the shutdown of entire healthcare facilities, putting patients' lives at risk. Ransomware attacks that lock access to critical healthcare IT systems often cause disruption that leads to cancelled outpatient appointments and elective surgical operations. In more serious attacks, emergency rooms have had to turn ambulances away or cancer centres have had to postpone treatment for their patients. More recently, there have been cyber-attack to steal mental health records where the attackers have ultimately published the confidential records online, demonstrating how cyber-attack can impact both the physical and mental well-being of the victims.

- To address the growing digital risk to health care, it is important to enhance cyber-maturity. Cybersecurity maturity is an organization's level of readiness to defend itself and its digital assets against cyber-attacks. This involves investing in people, processes and technology, including through cyber-awareness training and development of incident response plans to be rehearsed by staff in anticipation of a cyber-attack. It is critical to increase communication and collaboration with law enforcement agencies (e.g., police, INTERPOL), governmental agencies (e.g., cyber-security agency, public health institute, national agency for the safety of medicines and health products, nuclear safety agency), private sector and non-governmental organizations; these entities can provide alerts and warnings about ongoing cyber-attacks.

THERE IS A RANGE OF TACTICS PROPOSED TO COUNTER DISINFORMATION:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11 , November - 2025

- Raising awareness of disinformation and information manipulation.
- Promoting critical thinking
- Promoting digital, health, and scientific literacy programs
- Promoting trusted sources of information and voices of authority
- Supporting fact-checking activities, which include the use of fact-checking technologies and human fact-checkers
- Working with relevant stakeholders, such as the security sector, social media providers, law enforcement, cyber agencies, NGOs, and international organizations to tackle this new threat
- Identifying drivers of (mis)trust in populations, and how those drivers are exploited to create disinformation campaigns
- These drivers can inform long-term solutions to guard against disinformation
- When encountering new information, everyone should ask themselves:
  - Is this content reliable?
  - Who is the author?
  - What is the source of the claims?
  - Is the information outlet reliable?
  - How do I feel about this piece of information?

HEALTHCARE IS THE MOST VULNERABLE SECTOR

The healthcare (MED) sector has faced the highest number of data breaches compared to all other sectors, including financial, educational, and government organizations.

From 2005 to 2019, the healthcare sector accounted for 61.55% (3912 out of 6355) of all reported data breach incidents.

This vulnerability increased in the more recent timeframe of 2015-2019, during which the healthcare sector was the victim of 76.59% (1587 out of 2072) of all incidents.

Abstract

This documents the technical and security configuration of a critical e-Health application, based on a structured infrastructure and security assessment. The system is hosted in a private cloud environment, with its data center confirmed to be located in the safe and stable country. Network performance is underpinned by a robust multi ten Gbps internal traffic capacity featuring path redundancy, monitored by dedicated performance dashboards with defined saturation thresholds. Key connectivity to the e-Health database is established via a Private IPVPN. However, the assessment identifies crucial gaps in data governance documentation, with several critical compliance and security details—including confirmation of 100% in-country data storage, statutory retention periods, secure deletion/archival procedures, and audit logging for stored data—remaining pending from the application owner. This highlights the necessity of fully integrating application-level policies with core infrastructure capabilities for a complete security profile.

---

1. INTRODUCTION

The security and operational resilience of e-Health applications are paramount, directly impacting patient care and regulatory compliance. This paper outlines the fundamental infrastructure, network, and data governance parameters of a deployed e-Health system. The objective is to formally document the existing technical controls and identify areas where application-specific security policies must be clarified to complete the compliance posture. The assessment is structured around three core pillars: Network Performance, Hosting and Security Architecture, and Data Governance.

---

2. FINDINGS ON NETWORK AND INFRASTRUCTURE

A. Network Performance and Bandwidth Allocation

The network infrastructure is configured for high capacity and redundancy to ensure continuous system availability:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11 , November - 2025

- Allocated Bandwidth: The internal traffic capacity is established at a multi ten Gbps level, ensuring high throughput for application processes. This capacity includes path redundancy for resilience against network failures.
- Performance Monitoring: System performance is actively monitored via dedicated performance dashboards or tools to track bandwidth usage.
- Saturation Thresholds: Defined alert thresholds are in place to proactively notify administrators in the event of network saturation or abnormally high usage.
- Content Delivery Network (CDN): The system does not utilize a Content Delivery Network (CDN) to optimize performance, relying instead on the high internal network capacity.

B. Hosting Environment and Network Segmentation

The system is deployed within a secure and segregated environment, leveraging private cloud resources and network controls:

- Hosting Environment: The system is hosted within the STC private cloud environment.
- Connectivity to e-Health DB: Connectivity between the application and the core e-Health database is established using a Private IPVPN, ensuring a secure and isolated link for data exchange.
- Network Access Controls: Firewall rules or access controls are confirmed to be in place to segment traffic and restrict access between different network zones, enforcing the principle of least privilege.
- Segmentation Details (Pending): Specific details regarding the system's location (DMZ or internal network zone) and the existence of a dedicated admin zone for system management are pending confirmation from the application owner.

---

3. DATA GOVERNANCE AND STORAGE

The system's data residency meets initial requirements, but the audit revealed critical missing details regarding data lifecycle management and accountability.

- Storage Location: The primary data center location is confirmed to be in the Saudi capital, Riyadh.
- Data Residency (Pending): Confirmation that all data is stored fully inside Saudi Arabia is pending confirmation from the application owner.
- Data Retention (Pending): The defined retention period for backups or data before archiving or deletion is pending confirmation from the application owner.
- Deletion Procedures (Pending): Specific procedures for secure data deletion or record sealing after the retention period are pending confirmation from the application owner.
- Audit Logging (Pending): Confirmation on whether access logs are maintained for stored data (i.e., who accessed the data and when) is pending confirmation from the application owner.

Proposed Mitigation Strategies

The study reviews several advanced strategies that hospitals can use to lessen or prevent the effects of cyberattacks:

Proactive Incident Response (IR): A six-step process covering planning, detection, analysis, containment (e.g., sandboxing), recovery, and post-incident review.

Secure Architecture based on Blockchain and Artificial Intelligence (AI): A proposed multi-layered system that uses AI techniques (like Support Vector Machines) to check for security flaws and a Blockchain layer for secure data storage.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11 , November - 2025

Data privacy: Ensure HIPAA compliance by anonymizing ePHI before processing with gen AI and incorporating tokenization to avoid external dissemination of patient information.

Training: Create AI-driven cybersecurity training for healthcare providers to improve awareness, minimize security risks and meet compliance requirements.

Patch management: Implement an efficient, AI-driven patch management system to ensure that the most critical vulnerabilities are patched first and medical devices receive timely software updates.

Intrusion Detection Scheme: A framework relying on a Stacked Autoencoder for feature extraction and the XGBoost algorithm to determine if behavior is intrusive

Threat intelligence: Employ gen AI to analyze large amounts of data, detect and respond to potential threats to medical devices and deliver alerts to healthcare providers.

The XGBoost (eXtreme Gradient Boosting) algorithm is a highly effective machine learning model used in health cybersecurity primarily for cyber threat detection and Intrusion Detection Systems (IDS). Its speed, accuracy, and robust performance make it an ideal choice for protecting sensitive healthcare data and systems, especially those involving the Internet of Medical Things (IoMT).

Key Applications in Health Cyber Protection

XGBoost is leveraged to classify network traffic, system logs, and device behavior as either normal or malicious.

1. Intrusion and Anomaly Detection

XGBoost excels at classifying complex, high-dimensional data, which is typical of network traffic and system logs.

Real-time Threat Identification: The algorithm is trained on labeled data of normal and various attack types (like DDoS, phishing, malware, and IoT exploits). It can then analyze live network packets and device behavior to flag anomalies that indicate an ongoing cyberattack with high accuracy.

IoMT Security: In the Internet of Medical Things (IoMT)—which includes wearables, patient monitors, and smart hospital equipment—XGBoost is used to detect abnormal communication patterns or unauthorized access attempts that could compromise patient safety or data integrity. It can be implemented at the Fog Layer (e.g., a local server or gateway) to provide rapid, localized analysis.

2. Cyber Threat Classification and Severity Assessment

Beyond simple detection, XGBoost can categorize the nature of the threat, which is crucial for automated response systems.

Attack Type Classification: It can classify a detected intrusion into specific categories (e.g., identifying a threat as a Distributed Denial of Service (DDoS) attack versus a cross-site scripting (XSS) vulnerability).

Risk and Severity Scoring: By learning from historical incident data, the model can predict the severity level or likelihood of a cyber threat, allowing security teams to prioritize and allocate resources more effectively to the most critical risks.

Why XGBoost is Preferred in Healthcare

Healthcare environments present unique challenges due to the large volume of streaming patient data and the critical need for low-latency security measures. XGBoost's features directly address these needs:

High Accuracy: As an ensemble method, it often achieves superior accuracy and a high F1-score in detecting subtle attack patterns compared to traditional machine learning models.

Speed and Efficiency: Its implementation is optimized for parallel and distributed computing, allowing it to process massive volumes of network data quickly, which is essential for real-time threat detection.

Handling Class Imbalance: Cyberattacks are rare events compared to normal network traffic, leading to highly imbalanced datasets. XGBoost, often combined with techniques like hybrid random sampling, can effectively handle this imbalance to ensure high Recall (detecting true attacks).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11 , November - 2025

Explainable AI (XAI): Interpretability is a key requirement in healthcare. When paired with methods like SHAP, the XGBoost model can provide insights into which features (e.g., packet size, destination port, time of day) were most influential in classifying an event as a threat. This helps security analysts understand and trust the model's decisions.

HINT

A lot of security reports emphasize the necessity for the government to play an active role in bolstering cybersecurity measures for critical infrastructure, including healthcare. While he welcomed the federal government's initiative to establish cybersecurity goals for hospital organizations, he cautioned against imposing financial penalties for breaches. He argued that penalizing hospitals for breaches involving third-party vendors or partners doesn't address the core issue. Instead, he advocated for the adoption of voluntary cybersecurity standards as a more effective approach to enhancing security in the healthcare sector.

INCIDENT RESPONSE PLAN

As cyberattacks have become increasingly frequent and consequential in recent years, health facilities should prepare an incident response and business continuity plan. These plans should be regularly tested, exercised, and stored offline [55]. Plans should involve an agreed upon process with the appropriate stakeholders identified. It is important to have a designated team and a cybersecurity leader, or simply a designated person in cases where the organization does not have a CISO [56, 57]. The roles and responsibilities should be clearly divided within the team. The organizations should also have an agreement on what constitutes as a reportable incident and when to escalate [58, 59]. Ideally, plans should embed prevention training as well.

Incident response plans should also endorse post-incident steps. This can involve enforcing organization-wide password resets after an attack, factory resetting, and replacing compromised hardware and software as necessary. However, there needs to be an internal plan for regrouping and implementing changes [40]. The IT and cybersecurity system and its management should then be adapted to the new needs and requirements that were revealed by the incident (i.e., patching and beyond).

A notification system should be established between the health facility and the manufacturers [60]. A process can be built for those in the enterprise (e.g., clinicians, business administrators, and IT staff) to report incidents directly to the manufacturers. In fact, this type of sharing is also being mandated in the most recent FDA 510(k) pre-market submission guidelines.

INFORMATION SHARING

The exchange of potential threats, indicators of compromise, best practices, vulnerabilities, lessons learned, and of mitigation strategies between stakeholders across public and private sectors is an essential step in building the cybersecurity of healthcare systems. Information sharing facilitates situational awareness and a solid understanding of threats and threat actors, their motivations, campaigns, tactics, and techniques. Consequently, it better equips decision makers to understand organizational exposure and to employ enterprise risk management policies. Information sharing should include all stakeholders: providers, manufacturers, suppliers, payers, and electronic record providers, as well as government(s) where applicable. There are organizations that exist specifically to facilitate collaboration between institutions, for example, the National Health Information Sharing and Analysis

Privacy-Conscious Data Sharing and Processing

1. The Necessity of Sharing vs. The Barrier of Privacy

Need for Data Sharing: Sharing medical and genomic data is essential for effective patient care and advancing P4 medicine (Predictive, Preventive, Personalized, and Participatory medicine).

Privacy Barrier: The privacy risks associated with disclosing sensitive medical and genomic data have become a major barrier to the advancements of P4 medicine.

Stricter Regulations: This challenge is amplified by the evolution of stricter regulations like HIPAA (in the US) and GDPR (in the EU).

2. Solutions and Advantages

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11 , November - 2025

Advanced Technologies: The challenges can be overcome using advanced technologies, including cryptographic mechanisms (e.g., homomorphic encryption, secure multiparty computation) and strong trust distribution techniques (e.g., distributed ledger technologies).

Four Direct Advantages of These Technologies:

(a) Fine-Grained Access Control: They allow for more precise control over access permissions, reducing the need for privileged third-party accounts.

(b) Data Minimization: They help implement data minimization principles, releasing only the necessary data for an agreed-upon usage, which aligns with strict regulations and minimizes misuse risk.

(c) Data Confinement: Individual and identifiable data can be kept within the security perimeter of the governing medical institution.

(d) Distributed Logging & Resilience: They enable distributed logging and access control, which avoids single points of failure and greatly reduces the effect of a breach, while enhancing auditability and incident recovery.

RECOMMENDATIONS FOR CONNECTED MEDICAL DEVICES

1. The Scope and Risk of Medical Devices

Device Definition: The text uses the FDA definition of a medical device, which includes a wide range of equipment (IV pumps, monitors) as well as implantable (pacemakers) and connected devices (wearables like Fitbits).

Security Weak Links: These devices can act as weak elements in the security chain, propagating flaws or incidents and enabling malware to spread across the network.

Balancing Utility and Security: While these devices enable advancements like remote care, their utility and safety must be balanced with security and privacy.

2. Inherent Vulnerabilities and Limitations

Resource Constraints: Many devices lack proper security measures (like encryption or threat modeling) because they do not have the necessary battery power or built-in computing resources to efficiently employ them.

Outdated/Unsecured Design: Devices designed to function in isolation are often integrated into the network later. Additionally, their operating systems or platforms become outdated relatively quickly.

Physical Security: Physical security of wearable devices is often impossible due to their nature and short life spans.

3. Key Recommendation for Decision-Makers

Pre-Purchase Evaluation: Decision-makers should evaluate the expected lifetime of devices (e.g., manufacturer/vendor or OS support) before purchase.

Maintenance Policy: Hospitals and manufacturers must work together to develop a patching policy that minimizes equipment downtime.

Time Series Intervention Model

Time Series Data: This is the healthcare service use data (number of patient visits, etc.) collected sequentially over many time points (e.g., monthly). The data itself shows a historical pattern or trend.

Intervention: The attack on a health facility is the intervention. It is a specific, abrupt event that interrupts the normal time series.

Model's Purpose: The statistical model's job is to disentangle three things:

The baseline trend of patient visits (what would have happened without the attack).

The immediate effect of the attack (the sudden, steep drop in visits right after the event).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11 , November - 2025

The prolonged/sustained effect (how long the disruption, fear, or damage continues to suppress the number of visits in the weeks or months following the attack).

By using this model, the researchers were able to provide a quantitative measure (percentages) of the direct and lasting harm caused by the attacks, establishing a causal link between the violence and the disruption of health services.

CYBER INCIDENT TRACER (CIT)

The CyberPeace Institute has released a beta version of the Cyber Incident Tracer (CIT) #HEALTH, a unique platform that bridges the information gap between cyberattacks on healthcare and their impact on people. Knowing and understanding what is happening is the first step to taking action for global change.

CIT #HEALTH contains data on over 230 cyberattacks against the healthcare sector in over 33 countries. While this is a mere fraction of the full scale of such attacks on healthcare, it provides an important indicator of the rising negative trend and its implications for access to critical care. The incidents range from disruptive attacks, such as ransomware, to data breaches including account compromises from June 2020.

Beyond recording when and where attacks took place, the platform explores how they occurred and the extent of their impact on people and organizations. In the data analysed to date, over 14 million records were breached, including medical data, social security numbers, contact details, medical donor details, diagnostics, HIV status, financial information, corporate data, medical imagery, identity cards, and fertility status of patients. In incidents targeting patient care services (excluding laboratories) a minimum of 14% led to patients being redirected to other medical facilities and 19% to the cancellation of appointments.

Finally

Building the cyber resilience of a hospital is vital and it is a shared responsibility. Users (i.e., clinicians and administration staff) should undergo training and should practice digital hygiene, decision makers should enforce the proper policies and consider cybersecurity in purchasing decisions, and manufacturers should equip their products with the appropriate cybersecurity measures. The information security teams of hospitals should also enact and upkeep the proper tools to safeguard the hospital and patients.

Information security teams should equip users to counter social engineering methods by, for example, filtering e-mail content, auto-checking suspicious URLs in e-mails for linked malicious code, whitelisting trustworthy websites and applications, as well as blocking Flash, advertisements and untrusted JAVA code on the Internet, as necessary. Other tactics for reducing exposure should be used, such as intentionally changing default passwords and regularly updating security configurations on laptops, servers, workstations, firewalls, etc. Antivirus software is also important, along with penetration tests, control of physical access, and the maintenance of regularly updated backups (which should be stored offline). The organization’s website and the industrial control systems, including HVAC, cameras, fire alarm panels, should be secure and locked down from attacks. EDR Software can also help detect malware breaches and react properly to recorded infections. Finally, there should be appropriate tools in place for protecting data shared across different departments or medical institutions in a privacy-conscious way, therefore reducing the risk of intentional or unintentional breaches through trust distribution.

Adequacy of E-Health Network Infrastructure vs. Deficiency in Data Governance Documentation

The e-Health application is deployed on a highly resilient network infrastructure, featuring multi-gigabit (multi-ten Gbps) redundant bandwidth and leveraging a Private IPVPN for secure, sensitive database connectivity. Core network security is adequately managed through existing firewall rules and access controls.

Recommendations: Critical Documentation Deficiencies

However, the assessment identified a significant documentation deficiency in the area of Data Governance. The application owner must immediately provide confirmation and procedural documentation for the following four critical areas to achieve a complete security and compliance profile:

Full Data Residency Confirmation: Explicitly confirm that 100% of the system data is stored within Saudi Arabia, as required by local regulations.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11 , November - 2025

Data Lifecycle Management: Document the statutory data retention periods, define archival procedures, and detail the secure deletion/record sealing procedures.

Data Access Audit: Confirm that comprehensive access logs are maintained and auditable for stored data to ensure accountability and monitor for unauthorized access.

Network Zoning: Clarify the system's specific placement (DMZ/internal zone) and the status of a dedicated admin zone to fully validate network segmentation controls.

The completion of these pending items is essential for verifying compliance with local regulations and securing the application's entire data lifecycle.

Detailed Explanation of Critical Deficiencies

The listed deficiencies are fundamental to regulatory compliance and risk management, especially for a healthcare application dealing with sensitive patient data.

1. Full Data Residency Confirmation

What it is: A legal requirement in many jurisdictions (like Saudi Arabia) that mandates that all sensitive national data must be physically stored and processed within the country's geographical borders.

Why it's critical: This ensures that data is subject only to local privacy and sovereignty laws, which is a non-negotiable compliance requirement. Failure to confirm this immediately flags a major regulatory risk.

2. Data Lifecycle Management

This deficiency relates to formal procedures governing data from its creation to its disposal.

Statutory Data Retention: Healthcare regulations dictate how long specific patient records must be kept (e.g., 5, 7, or 10 years). The organization must clearly document these legal timeframes.

Archival Procedures: Formal procedures are needed for moving inactive data from active storage to secure, long-term archives. This saves operational costs and reduces the risk surface of the active system.

Secure Deletion/Record Sealing: This is the process of permanently destroying data at the end of its retention period, ensuring it cannot be recovered. For healthcare, "record sealing" might involve cryptographic methods to make patient data inaccessible while retaining a formal record of its existence. Without this documentation, the organization is legally exposed for improper data disposal.

3. Data Access Audit

What it is: The process of continuously recording and monitoring all actions performed on the application's data.

Why it's critical: Access logs are the primary defense for accountability and forensics. They allow security teams to:

Trace Actions: Determine who accessed, modified, or deleted data and when (e.g., "Nurse X accessed Patient Y's record at 2:00 PM").

Detect Unauthorized Activity: Identify patterns of suspicious behavior (e.g., a high volume of data requests from a single user) that could indicate an insider threat or a compromised account.

4. Network Zoning

What it is: The practice of logically dividing a network into separate security segments, or "zones," to contain threats.

DMZ (Demilitarized Zone): A buffer network containing public-facing resources (like web servers) that are exposed to the internet.

Internal Zone: The highly-protected network where sensitive resources (like the patient database) reside.

Dedicated Admin Zone: A highly secured, restricted segment used only by privileged users for managing the application and infrastructure.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11 , November - 2025

Why it's critical: Clarifying the system's placement and the existence of an Admin Zone is necessary to validate segmentation controls. Good segmentation ensures that if a public-facing component is compromised, an attacker cannot easily move laterally to the sensitive internal database.

Monitoring the Cyberattack" by IQVIA

(published March 22, 2024), provides an analysis of the impact of a significant cyber security event that occurred on February 21st, 2024, targeting a switch provider in the healthcare sector.

KEY FINDINGS AND SUMMARY

The document focuses on quantifying and analyzing the disruption caused by the attack on the U.S. healthcare system, particularly regarding prescription and medical claims data.

1. Impact on Prescription Data

Initial Drop: The attack led to an immediate, sharp drop in the volume of electronic prescription (eRx) transactions, peaking in the week ending March 1st.

Recovery and Workarounds: Pharmacies, patients, and other stakeholders quickly activated workarounds, such as shifting to paper prescriptions, phone calls, and using alternative switch providers.

Recapturing Volume: By the week ending March 15th, prescription volume began to recover, indicating that the system was quickly recapturing transactions that were initially missed or delayed due to the outage.

Drug Volume Shifts: Analysis showed significant volatility in dispensing volumes for certain drugs, particularly for those requiring Prior Authorization (PA), which were heavily impacted by the electronic disruption.

2. Impact on Medical Claims Data

Claims Lag: The attack caused a significant lag or "missing claims" in the medical claims data stream, reflecting the inability of providers to submit claims electronically.

Scenarios for Recovery: The report presents two illustrative scenarios for how the missing claims might be recaptured:

Bolus Scenario: A sharp influx of claims is submitted quickly once the system is restored.

Trickle Scenario: Claims are steadily entered over several following weeks.

Restatements: Regardless of the scenario, restatements based on the original service dates of the claims will be necessary to redistribute the volume appropriately and accurately reflect the timing of care delivery.

3. Glimpse of Resilience and Recommendations

The report concludes that the rapid response of various stakeholders—pharmacies, Pharmacy Benefit Managers (PBMs), and payers—helped to minimize what could have been a broad, catastrophic disruption.

KEY TAKEAWAYS FOR FUTURE RESILIENCE:

Activate Workarounds: Nimble facilitation of care delivery through contingency plans is crucial.

Patient Behavior: Patients demonstrated a willingness to invest in necessary treatments to avoid care gaps.

Contingency Planning: Investing in quick, effective, and patient-focused contingency plans is critical for all healthcare stakeholders.

Partnership: Coordination, clarity, and transparency between industry partners are essential to ensure individuals receive needed care in a crisis.

Conclusion: E-Health Assessment & General Recommendations

Adequacy of Network Infrastructure vs. Data Governance Deficiency

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 11 , November - 2025

The e-Health application is deployed on a highly resilient network infrastructure. The system features high-capacity, multi-gigabit (multi-ten Gbps) redundant bandwidth, uses a Private IPVPN for secure database connectivity, and has adequate core network security controls via existing firewall rules.

However, the assessment identified a critical documentation deficiency in Data Governance. To achieve a complete security and compliance profile, the application owner must immediately provide confirmation and procedural documentation for four key areas:

Full Data Residency Confirmation: Explicitly confirm that 100% of the system data is stored within Saudi Arabia to meet non-negotiable local regulatory requirements.

Data Lifecycle Management: Document statutory data retention periods, archival procedures, and secure deletion/record sealing procedures .

Data Access Audit: Confirm that comprehensive and auditable access logs are maintained to ensure accountability and enable forensic tracing.

Network Zoning: Clarify the system's specific placement (DMZ/internal zone) and the existence of a dedicated admin zone to fully validate network segmentation controls and prevent lateral threat movement.

The completion of these pending items is essential for verifying compliance with local regulations and securing the application's entire data lifecycle.

Broader Call for Cyber Resilience in Healthcare

The healthcare sector is a prime target for cyberattacks globally. These attacks, which include ransomware, not only threaten patient identity and finances but also impede hospital operations (e.g., cancelled appointments, postponed surgeries, ambulance diversions) and place the health and well-being of patients at risk.

Building cyber resilience is a shared responsibility. Recommendations to enhance overall cyber-maturity include:

Technology & Processes: Implementing advanced mitigation strategies like Proactive Incident Response Plans , AI-driven intrusion detection using algorithms like XGBoost , and adopting privacy-conscious data sharing technologies (e.g., homomorphic encryption).

People: Providing AI-driven cybersecurity training for staff , emphasizing good digital hygiene , and establishing strong information sharing channels among all stakeholders (providers, manufacturers, government).

Medical Devices: Decision-makers must evaluate the expected lifetime and manufacturer support of connected medical devices before purchase, and collaborate with manufacturers on patching policies to minimize downtime.

REFERENCES

[1] Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies Elham Abdullah Al-Qarni Department of Computing and Information Technology University of Bisha Bisha-Saudi Arabia
[2] Healthcare Data Breaches: Insights and Implications Adil Hussain Seh 1, Mohammad Zarour 2 , MamdouhAlenezi2, AmalKrishna Sarkar 1,3, Alka Agrawal 1, Rajeev Kumar 1,* andRaeesAhmadKhan1, 13 May 2020
[3] THE IMPACT OF CYBERATTACKS ON PATIENT SAFETY AND HEALTHCARE INFRASTRUCTURE: A RISK MANAGEMENT PERSPECTIVE, Eniola Akinola Odedina, Covenant University, 09, September-2021
[4] Impact and Aftermath of the Change Healthcare Cyberattack: Insights from the AHA, Rick Pollack, President and CEO, AHA, Published on: Thu, 4 Apr 2024
[5] Quantifying the effects of attacks on health facilities on health service use in Northwest Syria: a case time series study from 2017 to 2019, Ryan Burbach,1 Hannah Tappis ,2 Aula Abbara ,3 Ahmad Albaik,4 Naser Almhawish,5,6 Leonard S Rubenstein,7 Mohamed Hamze,4 Antonio Gasparrini,8 Diana Rayes,2 Rohini J Haar, 8 August 2024
[6] Monitoring the Cyberattack, Published March 22, 2024, U.S. Research & Insights, IQVIA