AL HABTOOR RESEARCH CENTRE

When Healthcare Data Becomes a Weapon of Geopolitical Competition

HABTOORRESEARCH.COM

2026
OCTOBER

AL HABTOOR RESEARCH CENTRE

Dr. Azza Hashem

Managing Director of Al Habtoor Research Centre

Prepared by

Sherif Amin

Political and Security Studies Researcher

Farah Aburaya

Political and Security Studies Researcher

Designed by

Abdelazem Mohamed

Senior Graphic Designer

This publication is free and not intended for sale or distribution. Its sale or distribution within or outside Egypt is prohibited without written permission from the Al Habtoor Research Center, which retains all intellectual property rights to the content.

Contents

HEALTHCARE DATA AND GEOPOLITICAL COMPETITION

Healthcare as a Strategic Asset 4

Healthcare Data Is Becoming a Strategic Asset 6

The Strategic Attack Surface 8

The New Strategic Attack 9

An Emerging Strategic Model 16

Access and Sovereignty 19

Strategic Dependence Without a Breach: Who Controls Access and Continuity? 20

The Middle East Healthcare Nexus 21

Governance and Resilience 25

Governance Recommendations 26

Conclusion 27

References 28

I. Healthcare as a Strategic Asset

Hospitals are increasingly becoming prominent targets for cybercrime. Ransomware, phishing, data theft, and sabotage are becoming more threatening as healthcare combines high-value information with extreme sensitive data. Healthcare data is becoming increasingly valuable as it becomes digitalised; hence, revealing biological characteristics, scientific capabilities, and societal resilience.

Accordingly, a hostile actor's objectives may extend beyond merely stealing records. "Hostile actor" combines criminals, intelligence services, commercial competitors, and state proxies. Depending on the actor and its aims, access to healthcare systems could be exploited to gather intelligence on the demographic formation of a competitor country, or its healthcare system's crisis response mechanisms, or clinical decision-making processes, or confidential scientific research.

An attacker may use this data to identify areas to disrupt healthcare infrastructure or paralyse the country's healthcare system for a geopolitical leverage, or manipulate results and decisions to target the population's health, or build upon the information to surpass in this area of research. These approaches differ in both intent and outcome. A financially motivated actor may seek extortion, an intelligence agency may aim to obtain information, while state-affiliated or other politically motivated groups may seek to create disruption or engage in strategic exploitation.

In this regard, healthcare systems are likely evolving from mere source of information into interconnected intelligence ecosystems. Electronic records are linked with laboratories, research platforms, cloud services, medical devices, pharmaceutical and biotechnology companies, and national health infrastructure. Data is continuously collected, processed, and translated into decisions. Hospitals are becoming a focal point in a system that defines the characteristics of populations, supply chains, and institutional capabilities. This interconnectedness does not necessarily mean that all cyberattacks on healthcare are geopolitically motivated, but it does create an expansion of potential motives and threat pathways through which access to healthcare systems can acquire strategic importance and can also produce systemic harm.

Therefore, the strategic implications extend far beyond the traditional objectives of stealing patient information or disrupting services for financial gain. A hostile actor might seek to collect biological data, identify sensitive research programs, monitor specific patient or researches, track hospital operational patterns, test AI systems in healthcare, or access such data through a service provider serving multiple institutions. Potential objectives range from financial extortion and intelligence gathering to preparing for future coercion, gaining a competitive advantage, influencing decisions, or creating disruption during times of crisis.

So, what if the next geopolitical target was not a military system, but a hospital? In other words, under what conditions can access to healthcare data or disruption of a health service become an instrument of interstate leverage? As healthcare transforms into an intelligence-gathering ecosystem, genomic databases, clinical systems, and medical technologies could reveal far more than just patient data, potentially serving as strategic leverage and becoming a geopolitical weapon.

This analysis identifies five conditions under which such strategic leverage might arise: First, it relates to an actor's actual ability to access or control sensitive data, vital systems, or essential services. Second, it depends on a substantial dependency on that data, technology, or service. Third, it associates with limited or slow-to-emerge alternatives that constraint the affected organization or state's ability to respond. Fourth, it depends on the existing of a political, policy, or a decision that can be influenced by the breach or disruption.

These conditions can arise through two distinct pathways. The first involves unauthorized access, such as data theft, the manipulation of AI systems in healthcare, or the disruption of network-connected medical devices and shared suppliers. The second relates to strategic dependency in the absence of a breach where legitimate access arrangements, foreign technology providers, cloud infrastructure, software updates, or supplier concentration can create vulnerabilities by enabling control over access and service continuity. In both cases, a distinction must be made between the existence of a potential source of leverage and the actual attempt to exploit it or the emergence of tangible political consequences.

Healthcare Data Is Becoming a Strategic Asset

Healthcare has become a prime target of cyberattacks, with reports indicating breaches, operational disruptions, and financial losses impacting healthcare systems across various regions. According to the ORDR Healthcare Cybersecurity Statistics 2026 Report, 739 healthcare breaches were reported in the United States in 2024, affecting more than 276 million records. From January to April 2026, a sum of 252 healthcare data breaches has been reported to OCR. Similarly, IBM's 2025 Cost of a Data Breach Report estimates the average cost of a healthcare breach at 7.42 million USD.

The growing digitisation of healthcare sector has led to an increased reliance on interconnected systems, digital platforms, and data-intensive technologies, thereby creating additional points of vulnerability to cyberattacks. While these developments enhance operational efficiency and interoperability, they also introduce vulnerabilities that could compromise the confidentiality of healthcare data, the continuity of medical services, and the integrity of clinical systems.

This issue has gained importance amidst escalating geopolitical tensions in the post-COVID-19 era. Cyberattacks are used by opposing sides of regional conflicts to disrupt and sabotage critical infrastructure. For example, Russia's Federal Security Service (FSB) carried out cyberattacks against the EU using methods of malicious activities such as cyber infiltration as well as sabotaging critical infrastructure, which impacted states such as France, Germany, Poland, Cyprus, the Netherlands, Austria, Slovakia, Romania, and Finland. Furthermore, the European Repository of Cyber Incidents (EuRepoC) recorded 351 significant attacks on healthcare facilities between 2022 and 2025, while the ENISA NIS Investment 2022 study estimated the median cost of a major security incident in the healthcare sector at 300,000 EUR.

These concerns are particularly significant in the Middle East, where investments in healthcare digitisation and the adoption of interconnected medical technologies can lead to increased reliance on digital infrastructure and external technology providers. As healthcare systems become increasingly digitally integrated, assessing their cybersecurity requires looking beyond the direct costs of data breaches to consider how security vulnerabilities, supplier dependency, and limited alternatives can create opportunities for these systems to be leveraged as tools of strategic pressure.

The increase in cyberattacks could be traced back to healthcare systems becoming more digitally integrated and offering sensitive data that can be leverage for intelligence targets. These data include:

1. Personal data

It includes patient personal information, medical histories, mental health records, as well as financial and insurance information. A hostile actor can achieve financial gains from this data through fraud, identity theft, and blackmail. Furthermore, personal information can facilitate social engineering and targeted coercion by disrupting services and risking patients' lives.

In general, a collection of medical records may reveal patterns in the health characteristics of specific population groups. However, the extent to which such data can support assessments on the population level depends on the area of coverage, representativeness, geographic distribution, and selection biases. For instance, a dataset from a particular hospital can't be considered a complete representation of the whole population. Therefore, its strategic importance lies not only in the information contained in individual records but also in the aggregation of such information covering a range of patient groups, representing a general pattern in the population-level, and correlating it with other aspects.

2. Biological data

It includes human genomic data, such as DNA sequences, genetic predispositions (likelihood of getting a disease due to genes), and population-level genetic health records. Genomic data supports disease diagnosis, cancer detection and treatment, gene therapy and drug development, infectious disease research, and public health surveillance.

The sensitivity of this data depends on the capability to be identified and linked with patients representing a population-level identification. For instance, genomic data may remain identifiable or re-identifiable, depending on the level of detail available, the presence of additional information, linking data, and the effectiveness of access controls. Emerging technologies, including AI, may enhance some re-identification capabilities, but these technologies are not necessary for all forms of linking. The strategic importance of genomic data lies in the ability of such data to be combined with other personal information to develop detailed profiles of individuals, support intelligence gathering or coercion, or contribute to the development of biotechnology and medicine.

3. Scientific data

It encompasses clinical trial data which includes research studies coming from testing medical, surgical, or behavioural interventions in patients. Its geopolitical importance lies in its ability to reveal a country's scientific trajectory, vulnerabilities in its research, and the treatments it might be capable of producing in the future.

The consequences of unauthorized access to such data vary depending on the nature of the information. Commercially sensitive research may reveal intellectual property or provide competitors with knowledge that would have required significant time and investment to develop. Whereas unpublished studies and clinical datasets may reveal critical research findings, patient characteristics, or the direction of ongoing medical programs. In certain cases, the information may be linked to research related to national security issue. Regardless, confidential or unpublished research shouldn't automatically be treated as classified national security material. Its strategic importance depends on the sensitivity of the research, who accesses it, and how the information is used.

4. System-level data

It includes operational, logistical, and administrative data. It includes supply chain patterns, inventory levels, hospital administration, activity records, billing transactions, hospital capacity, and departments workflows. This type of data is very significant as it describes the health system's capacity, locations, records, dealings, number of suppliers each service depend on, and the speed of response to incidents or epidemics.

System-level data can hold strategic value as it connects the work of clinics, hospitals, laboratories, pharmacies, specialists, emergency services, and medical imaging facilities. A hostile actor may access information or hack inside the system or infiltrate a vendor that supplies a network of hospitals causing shutdowns, disruptions, a flawed delivery, or create a deficit in supplies.

The strategic importance of healthcare data increases when different types of information are linked. Personal, biological, scientific, and systems datasets provide multiple dimensions to the same healthcare system: who is affected, what biological characteristics are present, what research capabilities are available, and how the system itself functions. Digitalisation connects these data to AI systems, digital twins, medical devices, cloud platforms, and external service providers. Therefore, the fundamental issue is not simply the possibility of healthcare data theft, but rather the conditions under which these different types of data are accessed, granting an actor the knowledge, access, or ability to influence healthcare services and decisions.

II. The Strategic Attack Surface

The New Strategic Attack

Interconnected datasets, technologies, and services create multiple distinct yet intertwined pathways, where access can serve as a powerful strategic tool. A breach in one part of the healthcare ecosystem could expose sensitive information, compromise the integrity of clinical decisions, disrupt essential services, or reveal dependencies that extend across healthcare institutions and borders. The following framework identifies five emerging, interconnected risk areas: genomic databases, healthcare AI, digital twins, connected medical devices, and healthcare supply chains. These areas should not be viewed in isolation as a security vulnerability in one can lead to vulnerabilities across the broader healthcare chain. For instance, a hospital might rely on a supplier with a compromised system which could cause disruptions within its own services. Similarly, a laboratory might secure its internal database but exchange data with an AI platform whose training or validation processes lack sufficient oversight which could potentially undermine the reliability of the outputs.

The strategic risks arise through two distinct pathways. The first is unauthorized compromise, where a party gains access to data, systems, or services through theft, hacking, manipulation, ransomware, or the exploitation of technical vulnerabilities. The second is strategic dependency without a breach, where healthcare organisations may grant legitimate access to foreign technology providers or specialists through contracts involving cloud infrastructure, electronic health records, AI applications, software updates, medical devices, or data processing.

Accordingly, the political implications of healthcare data extend beyond the sole risk of system breaches. A hostile actor could exploit unauthorised access to steal genomic information, poison AI training data, alter device functionality, or disrupt a shared resource. By contrast, legitimate commercial or legal arrangements can create dependency when a healthcare system relies on a provider that is difficult to replace, particularly where alternatives are scarce, switching costs are high, or data and infrastructure fall under foreign legal jurisdiction.

Evidence indicates the connection and interdependence between the different areas in the healthcare system, where an exposed risk in one area compromises other areas. The CLAROTY's State of CPS Security: Healthcare Exposures 2025 report found that 99% of the 351 healthcare organisations examined confirmed known exploited vulnerabilities (KEVs). Moreover, the IBM's Cost of a Data Breach Report 2025 found that it takes an average of 279 days for the healthcare sector to identify and contain a breach.

> Hence, the main issue extends beyond the mere protection of individual databases. It raises a critical question about what conditions turn access into influence over services or decisions? Digitisation and interconnectivity make access to data a risk as it enables an entity to acquire knowledge or exert influence over healthcare services and related decisions.

Table 1 | Risk domains and conditional strategic effects

Risk Domain	What It Contains	Primary Security Dimension	Potential Clinical Consequences	Conditional Strategic Effect
Genomic Databases	Genetic profiles and population-level genomic information	Confidentiality, integrity	Exposure of sensitive biological information or inaccurate genomic analysis	Population profiling, intelligence gathering, coercion, or biotechnology advantage
Healthcare AI	Training data, models, inputs and outputs	Integrity	Flawed diagnosis, treatment recommendations, or resource allocation	Manipulation of healthcare decisions and research outcomes
Digital Twins	Patient data, personalised treatment and predictive models	Confidentiality, integrity	Inaccurate prediction, diagnosis, or treatment recommendation	Influence over predictive healthcare decisions and treatment recommendation
Connected Medical Devices	Real-time patient, system data and device functions	Availability, integrity	Malfunction, treatment delay, misdiagnosis, or physical harm	Cyber-physical disruption, espionage, or wider service disruption
Health Supply Chains	Third-party vendors and suppliers, software, and cloud services	Confidentiality, integrity, and availability	Delayed treatment, shortages, or disruption across institutions	Multi-institution or cross-border leverage through shared dependencies

Source: Authors' analytical framework, reproduced from the supplied manuscript.

Genomic Data as a Strategic Intelligence

Genomic data supports population profiling, including disease diagnosis and gene change identification, analysis of genetic predisposition, precision medicine or personalised medicine using a patient's genes, and biomedical research. In such a context, genomic data could be used in intelligence targeting, military advantage, and biotechnology competition when its different categories are combined.

These categories include:

- Genomic information: genetic profiles, DNA sequences, and population-level genetic characteristics.
- Clinical and trial data: patient responses, treatment outcomes, and characteristics recorded during clinical research.
- Unpublished research: ongoing findings, research directions, and experimental results that may reveal emerging scientific capabilities.
- Diagnostic and analytical methods: techniques used to interpret biological and clinical information.
- AI models and bioinformatics tools: computational systems used to process, analyse, and interpret biological data.
- Research collaboration records: information about institutional partnerships, areas of cooperation, and the distribution of specialised expertise.

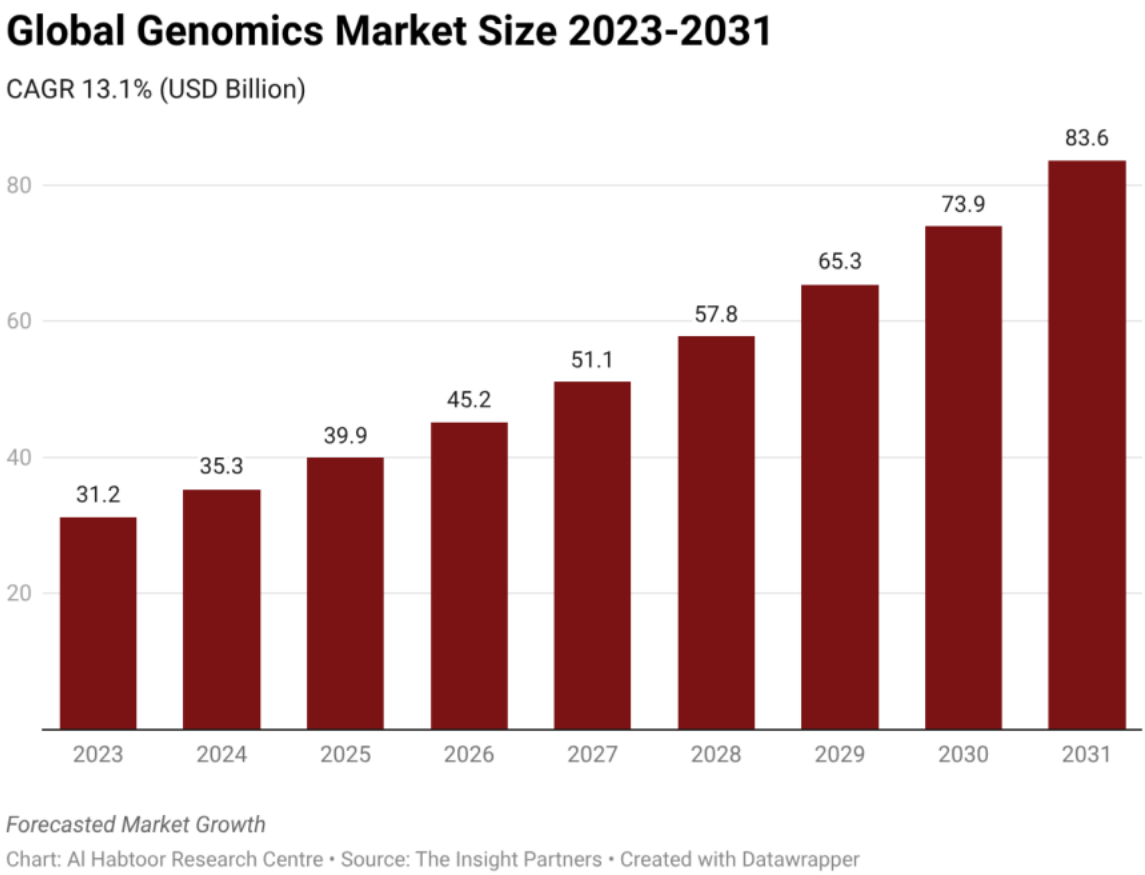
Each category has a different security and strategic value. Access to a large genomic database may reveal patterns within the populations and groups it covers, but the extent to which these patterns can support population-level generalisation depends on the database's coverage, representativeness, geographic distribution, and possible selection

biases. A large dataset doesn't automatically represent an entire national population. Nevertheless, healthcare institutions that store, process, and share highly sensitive, large-scale genomic databases may become more prone targets for cyber-attacks because of the volume, sensitivity, and potential correlation for the data they hold. The main strategic concern emerges when these categories can be accessed and linked to one another. For instance, genomic information could reveal genetic characteristics, while clinical data could indicate how specific conditions respond to treatment. When this data is combined with research records and analytical models, the resulting dataset can provide a more detailed picture of biological characteristics, research capabilities, and potential vulnerabilities than a single dataset could offer alone.

Such data could be compromised in several ways. First, data theft of genomic and clinical data, research findings, and metadata. This exposure of sensitive information might lead to espionage, intellectual property theft, and loss of competitive advantage. Second, ransomware and system disruption in laboratory IT, databases, and cloud platforms. This could cause interruption in diagnosis procedures and research, and disruption of surveillance programs that protects the whole network. More prominently is a hostile actor seeking to alter or manipulate genomic data without being detected. Such a compromise produces flawed results or errors in outcomes, which potentially leads to flawed or incorrect diagnostic or research decisions. Lastly, infiltration of a suppliers, cloud data, and shared research platforms. This gives indirect access to confidential biological data, hinder service provisions, and have greater access to the wider network of healthcare institutions that share a vendor or a cloud computing service.

Accordingly, a national genomic program must define which entities may access the data and which secondary users have access to data collection and processing. In addition, governments could co-models for technical security review, while engaging in national-level oversight.

Figure 1| Global genomics market size, 2023–2031



AI as a Tool for Decision Manipulation

Artificial intelligence (AI) in healthcare is increasingly influencing diagnosis, medical imaging, risk prediction, treatment recommendations, resource allocation, patient prioritisation, and documentation. The significance lies in the shift AI brought into the healthcare system, where it increasingly shapes what physicians see, which cases receive attention first, how resources are allocated, and service patterns.

A hostile actor does not necessarily need to have a direct access to the AI model itself to influence outcomes. Depending on the system architecture, manipulation could occur through different mechanisms, such as poisoning training data, modifying inputs during model usage, or compromising model update and validation processes. Distinguishing between these mechanisms is important as altered records do not automatically change a deployed model unless they enter a relevant training or update pathway. Consequently, the potential impact depends on how the AI system is deployed, the mechanisms for data validation and model updates, and whether an independent human review process is maintained.

The strategic implication for data poisoning is that the manipulated information may be incorporated into legitimate workflows, subsequently producing output that appear valid. For example, a scenario envisions an insider with access to data collection processes, such as in a laboratory or hospital, could introduce malicious samples into a dataset used for model training or updating. If such data enters the relevant training or validation process undetected, the model may learn the manipulated patterns and subsequently generate inaccurate outputs, potentially affecting diagnostic or treatment recommendations.

Therefore, a resilient healthcare AI program requires a comprehensive data protection chain addressing the AI lifecycle in order to avoid manipulation in training or validation stages in AI systems that could potentially produce biased or unsafe outcomes. The first step could be robustness testing of AI model against malicious tampering and data poisoning risks, as well as validation, prior to installation. After installation, any changes to training data, model parameters, or software updates must be validated before integration into the systems Continuous performance monitoring is also very essential to detect any signs of unexplained changes in the model behaviour. If an interference with medical AI systems is suspected, vast incidental reporting system should alarm on spot.

Digital Twins as a New Intelligence Layer

Digital twins are virtual representations of physical systems, processes, or individuals that can be updated using data from their real-world counterparts. In healthcare, their scope varies significantly. Digital Twins can simulate a patient's condition, provide personalised recommendations, predict disease risks or treatment effects, and support clinical decision-making. By continuously evaluating patient data in a virtual environment, digital twins can assess risks and predict complications. Thus, shifting treatment from reactive one to preventive and personalised one.

Moreover, "Digital twin" systems have been implemented in areas, such as hospital management, remote monitoring, and the diagnosis or treatment of health conditions, including chronic wounds and diabetes. Furthermore, more advanced Digital Cognitive Twins (DCTs) go further by employing AI to learn, predict outcomes, simulate options, and support or recommend decisions.

However, Digital Twins implementation remains limited, largely because the restricted access and share of health data, patient information confidentiality, and the heterogenous division of electronic health records. These issues complicate the development and deployment of digital twins in real clinical settings as this technology's effectiveness depends on improving data infrastructure, integrating it into clinical workflows, and ensuring sustained investment in the technology.

A healthcare digital twin model can integrate electronic health records, genetic and biometric information, clinical and demographic data, and incorporate physiological signals. Afterwards, the Digital Twins technology can help early detection of diseases before symptoms appear, predict the progression of conditions, and test various preventive or treatment options.

Given that digital cognitive twins integrate highly sensitive data, can become prone targets for cyberattacks. Consequently, the strategic concern extends beyond an unauthorized access to a specific patient record; instead, it encompasses access to, or the manipulation of, the digital models and data flows used to inform clinical or operational decisions. Depending on the system architecture, a hostile actor might attempt to steal sensitive information, manipulate data, alter model inputs, or interfere with the systems that generate predictions and recommendations.

So, the strategic implications depend on how the Digital Twins are utilised and which areas are affected. Most notably, when the same model or platform is used across multiple institutions, or when its outputs influence decisions of significant clinical or operational weight, or when independent verification or human oversight is insufficient, or the extent to which the manipulated information is shared with other systems or integrated into subsequent stages of the decision-making process.

In this regard, safeguarding measures need to include the protection of medical, genetic, biometric, behavioural, and psychological data confidentiality. Additionally, preserving data integrity becomes a necessity to prevent altering or manipulating records and data that could risk algorithmic bias which leads to flawed decision-making. Simultaneously, human auditing should be prioritised over inputs, predictions, outcomes, and automated recommendations. Furthermore, efforts would likely be directed towards testing models periodically and implementing stricter rules in hospitals and laboratories regarding data governance, privacy, and regulatory control.

Medical Devices' Vulnerability

Connected Medical Devices are technologies used for diagnosis, monitoring, treatment, and patient care support. They are capable of communicating with other devices, hospital networks, cloud computing services, and external software platforms. These devices range from implantable, such as pacemakers, and portable equipment, such as infusion pumps, to large-scale hospital systems, including MRI and CT scanners. They also encompass home care equipment, such as dialysis systems and blood pressure monitors, as well as wearables connected to mobile applications. In addition, these devices rely on cloud computing services, AI-driven software, and other systems connected to hospital networks.

The security of these devices is a shared responsibility throughout their lifecycle. Manufacturers are responsible for secure design, software integrity, vulnerability management, and secure updates. Healthcare providers are responsible for secure deployment, configuration, monitoring, and access management. While suppliers or cloud service providers may control additional infrastructure upon which device functionality depends.

Healthcare increasingly relies on cyber-physical systems, where any technological attack can impact patients, clinical workflows, and the overall medical environment. The strategic implications are associated with cyber-attacks that range from information theft to physical risks involving infusion pumps, patient monitors, connected diagnostic equipment, and wearable devices. When medical devices rely on cloud services, attacks targeting the cloud can impact devices and patients across multiple locations.

A hostile actor may attempt to compromise a device through various actions. During the manufacturing stage, malicious code could be injected into the software before the device reaches the healthcare provider. Once the device is being operated, attackers might target software update mechanisms or exploit vulnerabilities in connected systems. In cases where device functionality relies on cloud services, a breach of the supporting infrastructure could also impact the devices dependent on those services.

Regarding AI-powered medical devices, manipulation can occur at various stages. An attacker might attempt to "poison" training data, tamper with inputs during operation, or compromise the software used to reconstruct or interpret medical images and diagnostic systems. This could lead to a gradual decline in a device performance or produce flawed output that appear valid, leading to misdiagnosis or wrong treatment or delayed medical intervention, depending on the device's role and the availability of independent clinical verification mechanisms.

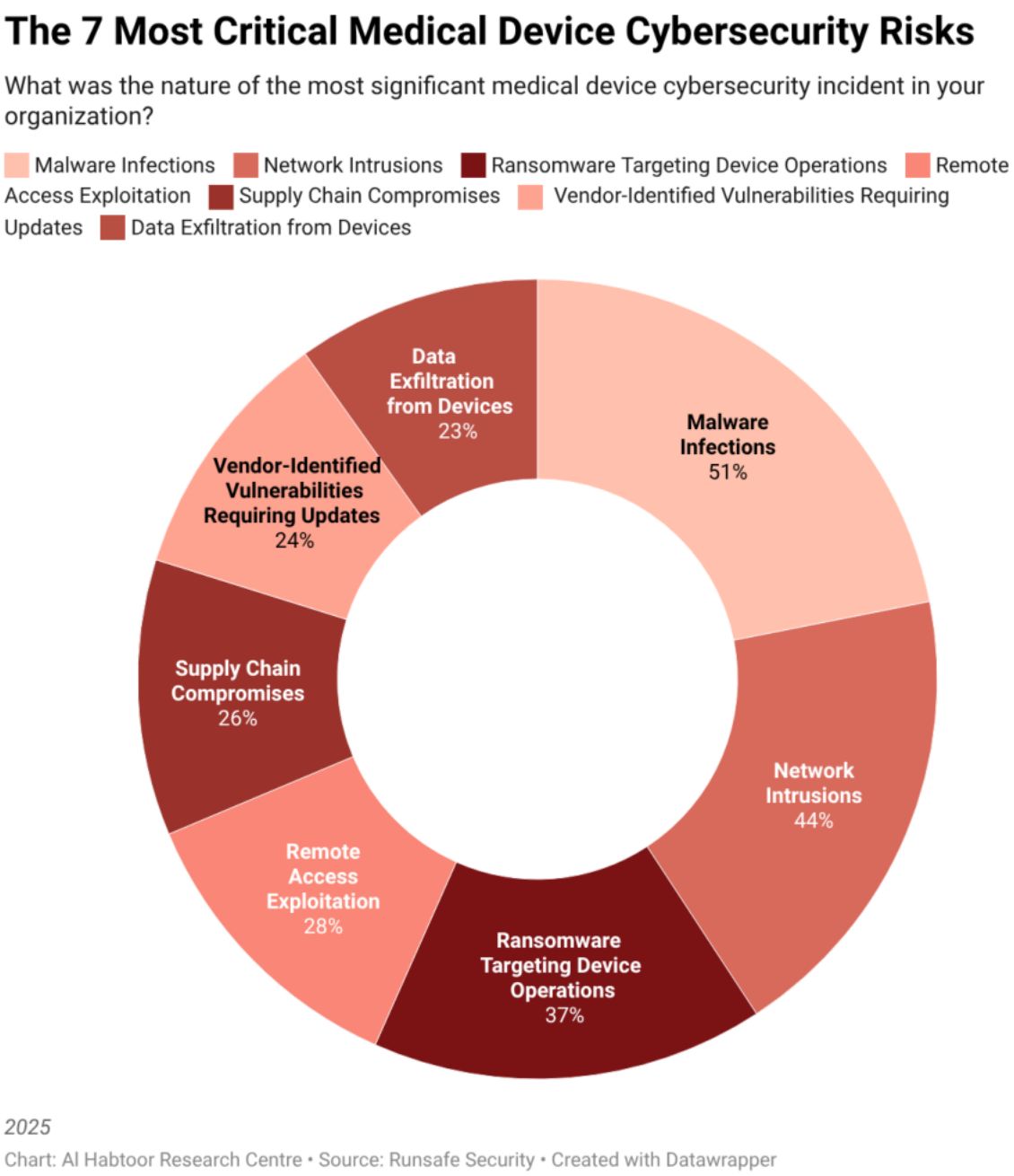
The security of connected medical devices is a shared responsibility throughout their lifecycle. Manufacturers are responsible for secure design, software integrity, vulnerability management, and secure updates. Meanwhile, healthcare providers are responsible for secure deployment, configuration, monitoring, access management, and incident response. Suppliers and cloud service providers may also control the infrastructure upon

which device functionality relies and must meet specific security requirements.

Accordingly, a device's security can't be assessed only at the time of purchase. Healthcare providers should treat secure update mechanisms, vulnerability disclosure practices, software provenance, and reliance on cloud computing as fundamental procurement criteria.

Across all five domains, healthcare institutions need to maintain continuous monitoring, incident-reporting and crisis procedures, periodic security testing, and defined emergency arrangements for compromised data, AI, device, cloud, or supplier services.

Figure 2 | Medical device cybersecurity incidents



Supply Chain and Systematic Exposure

The healthcare supply chain includes hospitals, clinics, health insurance, cloud service providers, software suppliers, medical device manufacturers, laboratories, pharmaceutical and biotechnology companies, and research institutions. World Health Organization (WHO) identifies these interconnected entities as part of a healthcare ecosystem vulnerable to cyberattacks.

The ongoing digitisation of medical infrastructure and its supply chains enhances efficiency but significantly expands the attack scope, making cyber-attacks more likely to spread beyond a single hospital or country. Hostile actors may not need to breach several hospitals; instead, they could target a single supplier serving hundred or a chain of hospitals.

The strategic implications reach multiple medical service providers and create shared security vulnerabilities cross-borders. A breach on a global medical device manufacturer, for instance, could disrupt the supply of surgical equipment and personalised medical implants, as well as it could expand geographically and delay surgeries in several countries connected to this supplier. For example, medical device manufacturer, Medtronic (based in Dublin, Ireland), was hit with a cyberattack that led to unauthorised access to the corporation's IT systems. It should be mentioned that Medtronic is responsible for developing devices for 70 health conditions while also catering to 150 countries around the world. While the attack did not directly impact any medical devices or patient safety, the attack exposed vulnerabilities in the company's cybersecurity structure. Had a cyberattack taken place on a manufacturing station or final products for operational use, the medical institutions who use Medtronic's products can be impacted as their patients would be at risk of being equipped with faulty medical devices or their personal data can be stolen by attackers.

Accordingly, hospitals require to strengthen their monitoring system for health-service providers, including inventories of suppliers, data flows, software vendors, and device interconnections. Moreover, contractual terms between medical services and suppliers should incorporate fundamental security clauses clearly defining security responsibilities, audit rights, liability for breaches, encryption standards, data location transparency, logging requirements, secure system update schedules, and comprehensive monitoring system covering all clients, capable of detecting attack patterns emerging across the whole chain.

In addition, over-reliance on a limited number of service providers can create cybersecurity risks within the healthcare sector. If a supplier supports data systems, cloud services, or clinical operations for several hospitals, a breach could compromise patient information or disrupt services at every organisation relying on that supplier. This can lead the disruption of clinical operations and treatment delays, as well as access to patient data, which can result in systemic paralysis. The extent of this disruption depends on the nature of the affected services, the number of dependent organisations, and the existence of effective continuity capabilities. This highlights the cybersecurity risks in shared dependency where a single vulnerability in the supply chain can have spill-overs affecting the entire healthcare chain. Furthermore, supplier concentration raises concerns regarding strategic dependency. In situations where alternatives are limited, switching costs are high, or systems are difficult to integrate, organisations may lack practical options to reduce their reliance on a specific provider.

An Emerging Strategic Model

Healthcare systems can become vulnerable to strategic compromise through two interconnected pathways: unauthorised compromise and strategic dependency without a breach. The first one involves unauthorised access to sensitive data, the manipulation of clinical or research systems, or the disruption of essential healthcare services. The second one arises when healthcare institutions rely on external technology providers, cloud infrastructure, software updates, medical devices, or data processing services that are difficult to replace or operate without.

Neither pathway automatically generates geopolitical leverage. The emergence of such

influence depends on a set of conditions, including the actor's ability to access sensitive information or influence critical services, the extent to which the affected institution or state relies on the data, technology, or supplier, and the availability of viable alternatives. In addition to the existence of a decision, policy, or political interest that could be impacted.

These pathways can intersect across five interconnected domains: genomic databases, AI in healthcare, digital twins, connected medical devices, and healthcare supply chains. A security vulnerability in one of these domains could compromise another due to shared data, software, infrastructure, or suppliers. For instance, a breach affecting a third-party platform could impact numerous healthcare organisations, while reliance on a single provider could disrupt service continuity even in the absence of a cybersecurity incident.

Table 2 | Healthcare incident severity framework

Severity	Clinical Impact	Institutional Reach	Duration	Recovery
Level 1: Low	No material clinical impact or patient-safety consequences	Isolated system or administrative function	Brief disruption	Routine restoration
Level 2: Moderate	Limited treatment delays or manageable clinical workflow disruption	One department or institution	Temporary disruption	Recovery through established procedures
Level 3: High	Significant disruption to clinical services or credible patient-safety risks	Multiple departments or a critical service within an institution, potentially several linked institutions	Prolonged disruption	Requires coordinated incident response and restoration
Level 4: Severe	Serious patient-safety risks, substantial treatment disruption, or confirmed patient harm	Multiple institutions or essential clinical services	Extended disruption	Recovery requires substantial intervention or alternative service arrangements
Level 5: Critical	Widespread severe patient harm or major impairment of essential healthcare capabilities	System-wide or cross-border disruption affecting interconnected healthcare services	Sustained disruption with limited immediate alternatives	Difficult recovery

Source: Authors' analytical framework, reproduced from the supplied manuscript.

Cyberattacks on the healthcare sector are likely to start from a vulnerable point, not necessary originated from a hospital. A hostile actor might compromise a cloud service provider, a genomic data processor, a medical device manufacturer, or an insurance company. The most vulnerable area to access facilitate collecting sensitive intelligence information; therefore, the actor could use the data for espionage or coercion or manufacturing national-level crisis, or even enhancing in the field themselves amid an intensifying geopolitical competition.

In this regard, the most dangerous scenario could involve an attack on a whole healthcare system, instead of a single system shutdown. A hostile actor could alter laboratory test results, profile population based on genomic database, manipulate input data for digital twins, or sabotage AI-powered medical devices. These attacks can lead to flawed results that appear to be credible on surface, such as misinterpretation of an emerging disease and

recommending inaccurate treatment. Here, detection is falling short, allowing the attackers to accumulate data or cause malfunctions across clinical decisions, research, resource allocation, and disease prevention policies. Consequently, national security becomes compromised when the healthcare infrastructure is attacked in an intended systematic intelligence level.

Hence, cyber threats in healthcare should be understood as a chain rather than a series of isolated technical incidents. Resilient national healthcare strategies, therefore, should combine all sectors of operations; supply chain network, medical device procurement process, independent verification of AI-powered services and cloud computing services, as well as software embedded in healthcare systems and high-risk or sensitive data. Additionally, continuous coordination on both institutional and cross-border levels becomes a necessity amid the rise geopolitical competition and the risks associated with it.

III. Access and Sovereignty

Strategic Dependence Without a Breach: Who Controls Access and Continuity?

Healthcare systems can become strategically dependent on third parties without suffering a security breach. A healthcare institution might legally share data with a technology service provider or rely on an external service, yet lack the practical ability to restrict data access, switch providers, or independently continue delivering essential care. While such dependency creates a potential leverage for influence or pressure, it does not automatically generate political pressure or guarantee its successful use. The fundamental question is whether this arrangement constrains the options available to the institution or government, particularly during crises, due to a lack of viable alternatives or the inability to adopt them in time.

To understand the concept of who controls the access and continuity of health data, it is important to understand the legitimate access as well as the research and secondary use of the data. In terms of legitimate access, hospitals and healthcare institutions are reliant on technology companies for ICT systems responsible for cloud infrastructure, electronic healthcare records, digital software, and AI applications. However, for these technologies to be utilised properly by both the technology suppliers and the medical institutions, the institution will have to provide legitimate access to health data. Naturally, due to sensitivity of health data, the transfer, use, and access of such data is heavily regulated to ensure legitimate access, data protection and fair use. This legality is also applied to research and secondary use rights of health data, as sensitive information from health data is being outsourced to a third-party for use outside of the scope of a healthcare facility. This can come in the form of medical research, government health reporting and monitoring, technology suppliers, and clinical care. As previously mentioned, the data is heavily regulated to ensure data protection, privacy, and protection from unauthorised access.

Control over healthcare data is distributed among various actors. Governments establish the legal framework governing data collection, processing, storage, research, and cross-border transfer. Healthcare institutions determine who may access the data and for what clinical or operational purposes, in accordance with these regulations and their own contractual obligations. Technology providers may process data under this authority, yet they can also restrict operational access through their platforms, software, cloud infrastructure, or maintenance arrangements. Hence, this chain represents an interconnected form of control over healthcare data.

Beyond control of legitimate access and secondary use being the responsibility of governments, the control of service operations, updates, and switching by technology suppliers cannot be overlooked. Technology suppliers have a significant hold over the operations of medical institutions, as they are responsible for providing these institutions with medical devices, cloud infrastructure, and software needed to manage healthcare operations and patient data. With the provision of such services, the technology supplier ends up with significant control over the medical supply chain, as medical facilities rely on these suppliers to maintain continuity of their systems and operations. This dependency on technology suppliers can lead to increased vulnerability for medical facilities, as if a technology supplier were to experience an outage or a disruption, the operations of the medical facility will also be disrupted thus resulting the collapse of the health supply chain.

Dependency becomes strategically important only under specific conditions: the service is essential, the provider exercises effective control over access to or continuity of the service, alternatives are unavailable or limited, and the organisation is unable to alter or maintain the service within an acceptable timeframe. For instance, if a hospital's clinical systems rely on software and cloud infrastructure provided by a specific vendor, the hospital may have limited scope to reject changes to the service or access arrangements if doing so would disrupt records, diagnostics, or treatment workflows. This represents a potential constraint on the institution's options, but it doesn't indicate that the provider has exploited this dependency for political purposes.

Now on an international level, controls over access and continuity of health data creates more avenues for increased vulnerability as the lines of control become blurred, especially during times of crisis. Health data may be subject to rules in multiple

jurisdictions, depending on where the data is stored, processed, or accessed, as well as relevant legal relationships. Disparities in national requirements regarding data protection, localization, and transfer can lead to routine compliance costs or delay data sharing. In public health emergencies or other crises, such restrictions can complicate cooperation if the parties involved can't readily determine the applicable rules or become uncertain whether a data transfer is permitted. However, the mere existence of regulatory disparities does not in itself constitute a tool of geopolitical leverage. The strategic implication lies in when the rules of a jurisdiction or its authority over a service provider, substantially affect data accessibility or the continuity of a vital service, particularly when affected institutions lack a timely alternative.

It also should be noted at cross-border data flows rules can also provide legal pathways for data sharing under specific circumstances. For example, the EU's Regulation (EU) 2022/2371 on serious cross-border threats to health allows for improved data sharing in the case of a public health crisis or an international threat. Although these laws make cross-border data flows easier in cases of emergency or international collaboration, countries around the world still employ stringent laws on cross-border data flows to maintain data sovereignty, which can be costly during a time of international crisis. Therefore, cross-border access becomes subject to jurisdictional control and data sovereignty laws even during times of crisis.

In terms of sovereignty, data localisation and data sovereignty mandates as well as investment in data infrastructure allows for countries to keep control over health-related data and essential services. However, a locally stored database might still rely on foreign software, cloud services, proprietary updates, or specialized support. Regarding innovation, partnerships between foreign governments can be beneficial to allowing healthcare facilities access to AI diagnostic tools, medical research, and expertise in emerging technologies. However, in the face of significant government restrictions, partnerships can slow down, which hinders research opportunities and access to data, which in turn slows down technological development. In terms of costs, building up domestic cloud infrastructure, technologies, and medical software can be a significant investment. Thus, the fundamental test lies not only in where the data resides, but in the ability of healthcare institutions to maintain essential care, transfer data legally, and switch service providers within an acceptable timeframe.

> This framework identifies dependencies in the Middle East that need closer comparison regarding: Who holds legal authority over access to health data? Which institutions and service providers exercise practical control? How does jurisdiction affect data flow or service continuity? And are there viable alternatives? These questions distinguish between routine commercial and regulatory dependencies and potential sources of strategic geopolitical leverage.

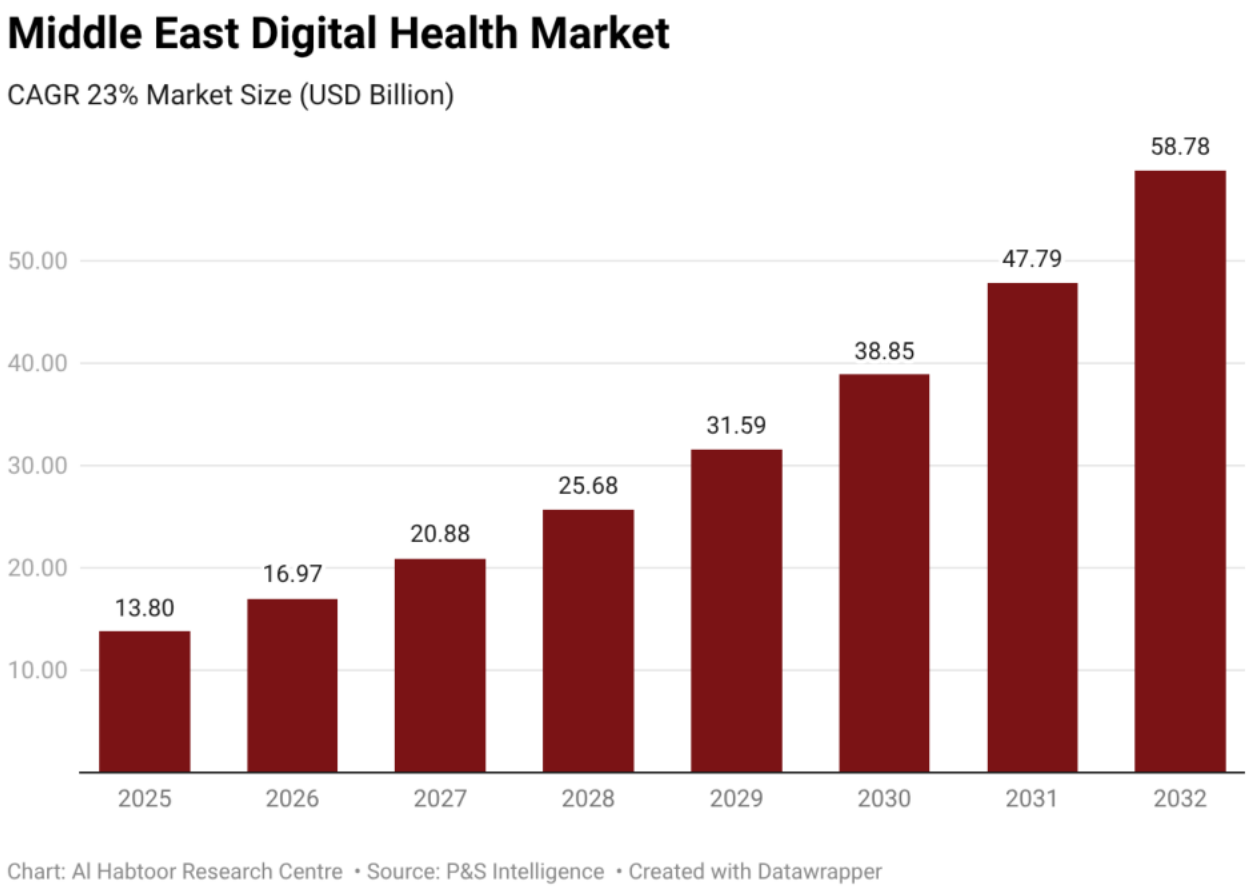
The Middle East Healthcare Nexus

Digitisation in the Middle East's healthcare sector, particularly in the Gulf region, is giving rise to new services while simultaneously creating interdependencies. Saudi Arabia and the United Arab Emirates have expanded their digital health infrastructure, while other Gulf states are investing in areas such as genomic medicine, robotics, and AI-enabled clinical services. The strategic issue here is not whether digital transformation automatically entails risks, but rather the extent to which control over sensitive data or critical services is concentrated, the ability of institutions to switch service providers or continue delivering care independently, and what the evidence and data reveal regarding these constraints.

Based on the healthcare data control matrix mentioned in the previous section, the UAE's health data law (Federal Law No. 2 of 2019) serves as a regional model for government regulations governing health data handling; Ministerial Resolution No. 51 of 2021 permits specific cross-border data flows for purposes such as overseas treatment, scientific research, clinical trials, and telemedicine. These measures demonstrate that legal sovereignty and operational control are interconnected yet distinct concepts.

For data usage may be subject to local regulations, while organizations remain reliant on external technologies or services. There is also UAE's Health Ministerial Resolution 51 of 2021, which allows for cross-border data flows under certain circumstances, such as "pharmacovigilance reporting, patient treatment overseas, the administration of insurance claims, scientific research and clinical trials, wearable healthcare monitoring devices, medical diagnostic testing, cooperation with UAE governmental institutions, telemedicine, for personal use, and other purposes as approved based on coordination with the federal Ministry of Health and Prevention."

Figure 3 | Middle East digital health market



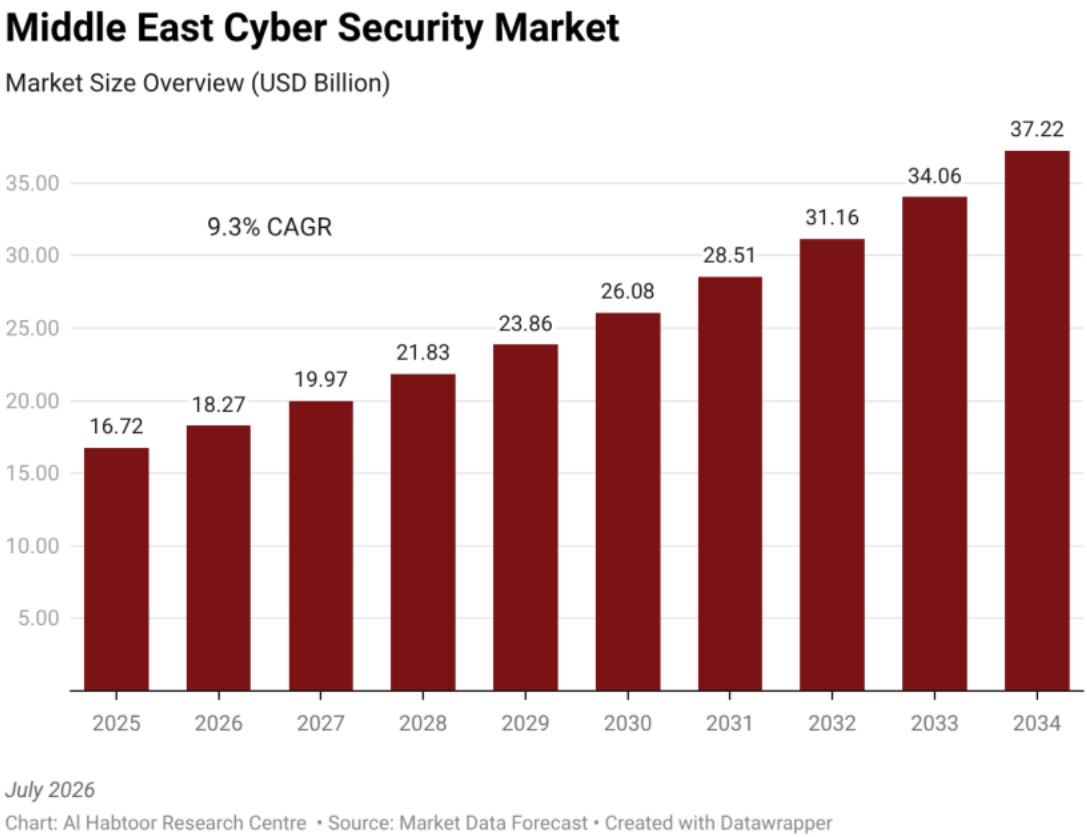
Publicly reported cyber incidents illustrate the trajectory of unauthorized comprise pathway, but should not be treated as evidence of dependence without a breach. For instance, a cyberattack carried out against U.S. medtech company Stryker by pro-Iran hacker group Handala on March 11th, 2026. The group attacked the company's internal Microsoft server, which impacted not only IT operations and data protection, but also could have potentially impacted patient care as well as the availability of devices. While Stryker is not a Middle East medtech company, Handala's cyberattack against the company shows how geopolitical tensions caused by the war on Iran extended beyond regional borders with the aim of disrupting U.S. healthcare sector, but it does not by itself demonstrate a direct clinical impact or successful coercion.

Potentially coinciding with geopolitical tensions, Middle East has been experiencing a rise in ransomware hacking from criminals. This is clear as "The Middle East has seen a surge in incidents involving ransomware, data theft, and the hijacking of connected medical devices. A prominent example was the cyberattack against American Hospital Dubai in June of 2025, in which ransomware was used to steal 450 million patient records and private information including Emirates ID numbers, credit/debit card information, personal addresses, and medical histories. Many attacks exploit legacy systems, outdated software, and a

lack of real-time monitoring". Such attacks leave the health data of individuals exposed which represents a significant breach of privacy and personal safety of patients and medical practitioners alike. These examples demonstrate why the attack method, the observed impact, and the political objective must each be assessed separately.

Despite the increase in cyberattacks with focus on healthcare institutions, states in the Middle East have worked to implement cybersecurity strategies to prevent and mitigate the impact of such attacks. The growth of the Middle East's cybersecurity strategies coincides with the digital transformations taking place throughout the region especially regarding the healthcare and finance sectors. As the Middle East continues to digitise, the surface for cyberattacks increasing, prompting these states to invest heavily in cybersecurity. According to Market Data Forecast, the Middle East cybersecurity market is set to be valued at $37.22 billion by 2034, which is double the estimated market value of $18.27 billion in 2026 (consider 9.3% CAGR). It should be noted that market expansion alone does not demonstrate reduced risk or policy success. Policy success or reduced risk stemming from increased investments must be observed through independent operational outcomes. These outcomes are achieved through cybersecurity laws and regulatory frameworks aimed at reducing the frequency of cyberattacks, while also protecting organisational or personal data. In the case of the Middle East, Saudi Arabia and the UAE have adopted stringent security laws and set up regulated frameworks to ensure the resilience of digital infrastructure across all government sectors including healthcare. The outcome of implementing successful cybersecurity policies and setting up robust regulatory frameworks can include "...fewer incidents that reach production impact, shorter dwell time, faster containment, better service restoration, lower loss from fraud or abuse, and improved confidence that critical controls are working". Through the increased investments, the Middle East states continue work towards providing greater security to local and regional digital infrastructure, which can prevent and mitigate potential cyberattacks on institutions such as the continuously digitising healthcare industry.

Figure 4 | Middle East cybersecurity market



Beyond investment, the Middle East states have incorporated cybersecurity into their national and digitisation strategies. The expansion of cybersecurity initiatives into national and digital strategies include strict policies as well as the establishment of regulatory frameworks to ensure that digital infrastructure across public sector industries is protected and regulated. This is clear as the "...protection of sensitive data, preventing financial loss, protection of national infrastructure, and preventing cyber espionage are key factors that accentuate the importance of a reliable cyber-security infrastructure".

Therefore, regional comparisons should focus on evidence of dependency and resilience rather than investment figures alone. While national cybersecurity bodies in Saudi Arabia and the UAE, along with health databases and digital health programs, reflect policy ambitions and institutional frameworks, projected growth in cybersecurity or healthcare markets indicates the need for risk reduction and infrastructure investment simultaneously. Operational indicators are required to include incident rates and their documented impacts, time of recovery, continuity of care during service disruptions, supplier concentration, contract and audit terms, as well as the time and cost required to replace a key service provider.

In the case of the UAE, the country has become a hub for cybersecurity initiatives through the establishment of regulatory bodies such as the Telecommunications and Digital Government Regulation Authority and the Cybersecurity Council. while also hosting several cybersecurity firms to help with the continuous digital transition. The primary goal of the TDRA goes beyond telecommunications regulation, as the stated mission focuses on leading in the ICT sector, while also promoting smart transformation in the UAE. This mission is also highly centred on the idea of boosting digital government, as the TDRA mentions their goal is also to always make digital services seamless and accessible for all persons, while also striving to be the number one nation in the provision of digital services. More importantly, the UAE Cybersecurity Council implements laws and sets up regulation frameworks aiming to boost confidence in digital infrastructure, while also protecting data, deterring individuals from committing cybercrimes, and assuring compliance with information assurance standards. This is clearly exemplified through Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes, aimed at penalising hacking and the spread of rumours as well as false information for the security of the nation, while Federal Decree Law No. 45 of 2021 on the Protection of Personal Data, is aimed at regulating how organisations use personal data as well as enforcing data protection.

In Saudi Arabia's case, cybersecurity frameworks were adopted across the financial sector and healthcare sectors to protect infrastructure while also promoting data protection and security, which is implemented by the National Cybersecurity Authority (Saudi Arabia). This has resulted in an expansion of the healthcare cybersecurity market in Saudi Arabia, as the market is expected to increase from $540 million in 2023 to $1.65 billion in 2032 (15% CAGR). Moreover, countries such as Qatar, Bahrain, Oman, Israel, and Egypt have invested heavily on cybersecurity initiatives, which shows how the region is striving to lead the world on issues relating to cybersecurity and digitisation.

IV. Governance and Resilience

IV

Governance Recommendations

Effective governance must address two distinct sources of risk. First, when a system is compromised, institutions need to detect the incident, contain its impact, protect patients, and restore essential services. Second, when risks arise from legitimate dependencies, institutions need to regulate access to data and systems, asses supplier relationships, and ensure continuity of care or the ability to switch providers if access or service is interrupted. While these pathways may overlap, the occurrence of a cyber incident or the existence of a dependency does not, in itself, imply political intent or the successful coercion.

In such as context, responsibility is distributed across four levels. National authorities establish common rules, receive incident reports, and coordinate responses. Healthcare institutions safeguard clinical operations and ensure continuity of care. Suppliers commit to securing the products and services they provide and cooperating during incidents. Regional partners facilitate information sharing and mutual assistance.

Table 3 | Governance responsibilities across four layers

Layer	Accountable Actors	Functions
National Layer	Health ministry, national cyber authority, research and security bodies	Data classification, incident reporting, genomic data process oversight, and national health cybersecurity framework
Institutional Layer	Hospitals, laboratories, universities, clinics and public-health agencies	Hospitals security framework, data backups, AI and medical device assurance, and ensure continuity of clinical operations
Supply-Chain Layer	Cloud providers, software vendors, device manufacturers, laboratories and contractors	Supplier risk assurance, software and cloud computing control, data-sharing protection agreements, and incident cooperation
Regional Layer	Coordination between Arab and Middle Eastern health and cybersecurity agencies	Risk indicators sharing, cross-border exchange training programs, mutual assistance and crisis communication mechanisms

Source: Authors' analytical framework, reproduced from the supplied manuscript.

Organisations need to conduct periodic drills simulating incident scenarios, such as loss of access to records, compromised AI outputs, medical device failure, or the infiltration of a shared supplier. These proactive drills should determine whether staff can detect and escalate incidents, whether clinicians can safely continue providing essential care, the speed of service restoration, and which entity assumes leadership if multiple organizations are affected.

Similarly, procurement and suppliers share load of responsibility. Contracts and technical arrangements need to clearly specify terms for data access and secondary use, define obligations regarding security and updates, guarantee audit and incident notification rights, and clarify mechanisms for transferring data and services or terminating contract. On the regional level, Middle Eastern countries could enhance institutional cooperation regarding information-sharing about emerging cyber threats, direct more investments in medical and security research, and on the long-term, the countries could develop a regional regulatory framework that list certain security criteria for health institutions to operate. For instance, compliance safety prerequisites regarding medical devices and healthcare AI systems or software.

Hence, governments need to treat AI in healthcare and digital twins, software providers, and third-party suppliers as a matter of national

security, protecting their database and raising accountability. Beyond the national security designation, governments also need to translate patient autonomy and scientific collaboration into proportionate access, independent oversight, accountability, and secure research-sharing arrangements. However, with excessive regulation comes excessive costs of providing healthcare in a digital age. This includes increased financial costs, regulatory lag, as well as accountability opacity, especially when it comes to AI error, and ecosystem fragmentation and interoperability.

In sum, governance should be evaluated based on operational outcomes and proactive measures to mitigate unauthorised accessed and strategic dependency. Relevant indicators could include the time taken to detect, contain, and recover from incidents. Case by case evaluation is essential to determine the motive behind the incident whether it is a security vulnerability or a intended geopolitical coercion act.

Conclusion

Healthcare systems can become sources of strategic leverage through two interconnected pathways: unauthorised compromise and strategic dependency without a breach. The first pathway involves unauthorized access to sensitive datasets, the manipulation of clinical or research systems, or the disruption of healthcare services. The second pathway arises when hospitals, laboratories, or national health systems rely on external entities for technology, software, cloud infrastructure, medical devices, or hard-to-replace suppliers. Whether involving genomic databases, clinical research, AI, digital twins, network-connected medical devices, or supply chains, these pathways can lead to the exposure of sensitive information regarding the population and health system capabilities, or compromise the continuity of essential services. Consequently, the risks facing healthcare extend beyond data theft and ransomware attacks to encompass the potential for control over information, technology, or service delivery to impact the operations of healthcare institutions.

However, unauthorised compromise or strategic dependency without a breach does not automatically translate into geopolitical leverage. Such leverage requires access to sensitive information or control over a critical service, limited practical alternatives for the affected organisation or state, an actor capable of exercising that access or control, and a political decision or interest that could plausibly be influenced. The cases examined in this study illustrate how healthcare data, digital systems, and interconnected supply chains can create opportunities for espionage, manipulation, or disruption. Yet, these cases do not in themselves prove that every security vulnerability reflects geopolitical intent, or that every incident produces strategic leverage, or that an actor has successfully coerced a government.

The central uncertainty lies in whether, and under what circumstances, these technical and institutional dependencies might be deliberately exploited to influence political decisions or coerce national responses. For Arab states and the wider Middle East region, the priority is to bolster healthcare resilience without compromising patient autonomy, the quality of clinical services, scientific collaboration, or technological advancement. This requires proportionate oversight, accountability for AI systems and third-party service providers, secure research-sharing arrangements, and coordinated early-warning and response mechanisms capable of safeguarding clinical services.

Ultimately, the strategic question extends beyond whether an actor can access healthcare data or disrupt hospital operations. More precisely, it concerns whether such access or control, combined with limited alternatives and a politically significant leverage point, can be weaponised as a tool of coercion. Technical capability alone does not prove malicious intent or successful coercion; instead, assessing such a shift requires evidence regarding the actor's behaviour, the consequences for healthcare services, and any tangible impact on political decision-making.

References

Abtahi, Farhad. (2026). Data Poisoning Vulnerabilities Across Health Care Artificial Intelligence Architectures: Analytical Security Framework and Defense Strategies. Journal of Medical Internet Research, 28. https://www.jmir.org/2026/1/e87969

Ahmed, Mostafa. "Digital Cognitive Twins: The Hidden Face of the Data War." Al Habtoor Research Centre. November 3, 2025. https://www.habtoorresearch.com/programmes/digital-cognitive-twins-data-war/

Al Nuaimi, Dina, and Niyi Awofeso. (2025). The Value of Applying Big Data Analytics in Health Supply Chain Management. F1000Research, 13, 1237. https://doi.org/10.12688/f1000research.156525.4

Alder, Steve. "Healthcare Data Breach Statistics – Updated for 2026." The HIPAA Journal. September 4, 2026. https://www.hipaajournal.com/healthcare-data-breach-statistics/

Alkhattabi, Khalid. (2026). An adversarial-resilient intrusion detection framework for internet of medical things (IoMT) using digital twin-enabled behavioral threat modeling and federated hybrid ensemble learning. Scientific Reports, 16 (26532). https://doi.org/10.1038/s41598-026-55893-z

Alzoubi, Osama. "Rising cyber threats in Middle East healthcare: The urgent need for IoT and IoMT security." Middle East Health. December 16, 2024. https://middleeasthealth.com/medical-specialty-features/medical-cybersercurity/rising-cyber-threats-in-middle-east-healthcare-the-urgent-need-for-iot-and-iomt-security/

Bayerlein, Michael, et al. "Cybersecurity in the Healthcare Sector." Stiftung Wissenschaft und Politik (SWP). SWP Comment 2026/C 35, August 24, 2026. https://www.swp-berlin.org/en/publication/cybersecurity-in-the-healthcare-sector

CENSINET. "14 Cybersecurity Clauses for Healthcare Vendor Contracts." December 13, 2025. https://censinet.com/perspectives/cybersecurity-clauses-healthcare-vendor-contracts

Chase, Melissa, et al. "Cybersecurity Risk Analysis for Medical Devices in the Era of Evolving Technologies." MITRE (April 22, 2026). https://www.mitre.org/news-insights/publication/cybersecurity-risk-analysis-medical-devices-era-evolving-technologies

Cheriyan, Dr George. 2024. "How Digital Innovation Is Reshaping Middle East Healthcare." World Economic Forum. October 8, 2024. https://www.weforum.org/stories/health-and-healthcare-systems/digital-innovation-reshaping-healthcare-middle-east/.

CLAROTY TEAM 82. "State of CPS Security: Healthcare Exposures 2025". https://web-assets.claroty.com/resource-downloads/state-of-cps-security-healthcare-2025.pdf

Emirates News Agency-WAM. 2026. "Digital Health in UAE: An Integrated Ecosystem Enhancing Care Quality and Service Efficiency." Www.Wam.Ae. July 3, 2026. https://www.wam.ae/en/article/c11agy8-digital-health-uae-integrated-ecosystem-enhancing.

European Union Agency for Cybersecurity (ENISA). "ENISA Threat Landscape: Health Sector." July 5, 2023. https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf

European Union. 2022. "Serious Cross-Border Threats to Health | EUR-Lex." Eur-Lex.Europa.Eu. 2022. https://eur-lex.europa.eu/EN/legal-content/summary/serious-cross-border-threats-to-health.html.

Fahmy, Emad. "The future of cybersecurity in healthcare from a Middle Eastern perspective." WHX Insights. April 23, 2025. https://www.worldhealthexpo.com/insights/healthcare-management/the-future-of-cybersecurity-in-healthcare-from-a-middle-eastern-perspective

"Federal Decree-Law of 2021 on Countering Rumors and Cybercrimes Federal Decree-Law No. (34) of 2021 On Countering Rumors and Cybercrimes." 2021. https://uaelegislation.gov.ae/en/legislations/1526/download.

Flinders, Mesh, and Ian Smalley. 2024. "What Is Data Sovereignty? ." Www.Ibm.Com. June 3, 2024. https://www.ibm.com/think/topics/data-sovereignty.

Fortra. 2024. "The 7 Most Dangerous Healthcare Cyber Attacks | Fortra." Fortra.Com. February 2, 2024. https://www.fortra.com/blog/most-dangerous-healthcare-cyber-attacks.

Gibson, Ben, Masha Ooijevaar, and Kate Corcoran . 2025. "Data Protection and Cybersecurity Laws in UAE | CMS Expert Guide." Cms.Law. October 8, 2025. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/uae.

Gnanaprakasam, Pandian. "Healthcare Cybersecurity Statistics 2026 Report." ORDR. April 3, 2026. https://ordr.net/blog/healthcare-cybersecurity-statistics-2026-report

Gurbanov, Yunis. 2026. "Below Article 5: Europe's Collective Response to Russia's Gray-Zone War." Geopolitical Monitor. September 30, 2026. https://www.geopoliticalmonitor.com/eu-hybrid-threat-response-below-article-5/.

Harpur, Rebecca. 2025. "Malware vs Ransomware: Key Differences and How to Stay Safe." BlackFog. May 27, 2025. https://www.blackfog.com/malware-vs-ransomware-key-differences-and-how-to-stay-safe/.

Henry, Kevin. 2026. "Phishing Attacks in Healthcare: Examples, Risks, and How to Prevent Them." AccountableHQ. Accountable. April 6, 2026. https://www.accountablehq.com/post/phishing-attacks-in-healthcare-examples-risks-and-how-to-prevent-them.

IBM. (2025). "Cost of a Data Breach Report 2025 The AI Oversight Gap." https://na.ingrammicro.com/Ingram/media/North-America-US/EN-US/I/ibm/docs/IBM-cost-of-a-data-bre

ach-2025-full-report.pdf

InCountry Staff. 2024. "Essentials and Challenges of Healthcare Data Sovereignty Laws." InCountry. October 28, 2024. https://incountry.com/blog/essentials-and-challenges-of-healthcare-data-sovereignty-laws/.

International Trade Administration . 2024. "United Arab Emirates Regulations Limit Cross Border Health Data Flows." International Trade Administration . January 22, 2024. https://www.trade.gov/market-intelligence/united-arab-emirates-regulations-limit-cross-border-health-data-flows.

INVAMED. 2026. "The Critical Challenges Facing Healthcare Supply Chain Management." Invamed. February 22, 2026. https://invamed.com/news/the-critical-challenges-facing-healthcare-supply-chain-management.

Javed, Moeeza . 2024. "Cybersecurity Strategies of MENA Countries – MEPEI." Mepei.Com. July 21, 2024. https://mepei.com/cybersecurity-strategies-of-mena-countries/.

Jones, Tim, Shabnam Karim, Simon Lamb, and Sajeedah Bari. 2026. "Heightened Cyber Risks in the Middle East: Geopolitical Tensions Fuel Digital Conflict." Data Protection Report. March 5, 2026. https://www.dataprotectionreport.com/2026/03/heightened-cyber-risks-in-the-middle-east-geopolitical-tensions-fuel-digital-conflictintroduction/.

Kalleklev, Arve Johan, and Peter Hellström. 2026. "Managing Supplier Risk in Healthcare Cybersecurity." DNV. June 15, 2026. https://www.dnv.com/cyber/insights/articles/managing-supplier-risk-in-healthcare-cybersecurity/.

Kaspersky. (2024). "Whispers from the Dark Web Cave - Cyberthreats to the Middle East." https://content.kaspersky-labs.com/se/media/en/whispers-from-darkweb.pdf

Kaspersky. 2026. "Your Healthcare Data: Who Has Access and Why?." /. August 5, 2026. https://me-en.kaspersky.com/resource-center/b2b/your-healthcare-data-who-has-access-and-why.

Katsoulakis, Evangelia, et al. (2024). Digital twins for health: a scoping review. npj Digital Medicine, 7(77). https://doi.org/10.1038/s41746-024-01073-0

KMS Technology. "7 Types of Healthcare Data: A Comprehensive Overview." December 22, 2025. https://kms-technology.com/blog/types-of-healthcare-data-a-comprehensive-overview/

Kohut, Mykhaylo. 2026. "IoT in Healthcare: Key Benefits and Use Cases." Software Development Company - N-iX. February 23, 2026. https://www.n-ix.com/iot-healthcare-key-benefits-use-cases/.

Lindquist, Margaret. 2026. "What Is Digital Transformation in Healthcare?." Oracle.Com. Oracle. May 7, 2026. https://www.oracle.com/middleeast/health/digital-transformation-healthcare/.

Lumenova. 2025. "Data Poisoning Attacks: How AI Models Can Be Corrupted." Lumenova AI. August 15, 2025. https://www.lumenova.ai/blog/data-poisoning-attacks/.

MacAlpine, Maggie. 2025. "Cybersecurity in Middle Eastern Healthcare: Protecting Patients in a Digital Age." Seceon Inc. May 7, 2025. https://seceon.com/cybersecurity-in-middle-eastern-healthcare-protecting-patients-in-a-digital-age/.

Market Data Forecast. 2026. "Middle East Cyber Security Market Report." Market Data Forecast. July 2026. https://www.marketdataforecast.com/market-reports/middle-east-cyber-security-market.

National Institute of Standards and Technology. "Artificial Intelligence Risk Management Framework (AI RMF 1.0)." (NIST AI 100-1). (U.S. Department of Commerce, January, 2023). https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

Non-Human Identity Management Group. 2026. "Cybersecurity Outcomes." NHI Management Group. September 20, 2026. https://nhimg.org/glossary/cybersecurity-outcomes/.

OECD. "Building and sustaining collaborative platforms in genomics and biobanks for health innovation." (OECD Science, Technology and Industry, March 2021, No. 102). https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/03/building-and-sustaining-collaborative-platforms-in-genomics-and-biobanks-for-health-innovation_13abb85e/11d960b7-en.pdf

Office of The Director, National Institutes of Health (OD). "Request for Information on Proposed Updates and Long-Term Considerations for the NIH Genomic Data Sharing Policy." (NOT-OD-22-029, November 30, 2021). https://grants.nih.gov/grants/guide/notice-files/NOT-OD-22-029.html

Petit, Zelie. "The Strategic Imperative of Biotechnology: Implications for U.S. National Security." Center for Strategic and International Studies (CSIS). September 27, 2024. https://www.csis.org/blogs/strategic-technologies-blog/strategic-imperative-biotechnology-implications-us-national

Ringeval, Mickaël, et al. (2025). Advancing Health Care With Digital Twins: Meta-Review of Applications and Implementation Challenges. Journal of Medical Internet Research, 27, e69544. https://doi.org/10.2196/69544

RuneSafe Security. 2025. "The Top 7 Medical Device Vulnerabilities Of 2025." RunSafe Security. September 4, 2025. https://runsafesecurity.com/blog/top-medical-device-vulnerabilities/.

Sention. "Genomic Data Has Become a Strategic Asset: Why High-Risk Laboratories Need to Act Now." June 30, 2026. https://www.sention.co/threat-update/genomic-data-has-become-a-strategic-asset-why-high-risk-laboratories-need-to-act-now

Shadadi, Ebtesam, et al. (2025). Exploring Cybersecurity and Phishing Attacks within Healthcare Institutions in Saudi Arabia: A Narrative Review. World Academy of Science, Engineering and Technology - International Journal of Computer and Information Engineering, 19 (4). https://www.researchgate.net/publication/391213234_Exploring_Cybersecurity_and_Phishing_Attacks_within_Healthcare_Institutions_in_Saudi_Arabia_A_Narrative_Review

Shahnazinia, Sara, et al. (2026). Healthcare digital twins: A methodological literature review on integrating IoT and AI for personalized medicine and predictive care. Telematics and Informatics Reports, 22. https://doi.org/10.1016/j.teler.2026.100325

Shen, Mei-di, et al. (2024). The effectiveness of digital twins in promoting precision health across the entire population: a systematic review. npj Digital Medicine, 7 (145). https://doi.org/10.1038/s41746-024-01146-0

Simmons & Simmons. 2019. "Simmons & Simmons." Simmons-Simmons.Com. May 20, 2019. https://www.simmons - simmons.com/publications/ck0b3wuarnuml0b85ffnosaz0/160519-new-health-data-protection-law-in-the-uae.

Sollof, Jordan. 2026. "Medical Device Supplier Medtronic Hit with Cyber Attack." Https://Www.Digitalhealth.Net/. Digital Health. April 28, 2026. https://www.digitalhealth.net/2026/04/medical-device-supplier-medtronic-hit-with-cyber-attack/.

Sullivan, Natalie, and Kristin Raphel. 2024. "Clinical and Hospital System Emergency Management Implications of Cyberthreats." Proceedings of the 2024 Workshop on Cybersecurity in Healthcare, November, 11–16. https://doi.org/10.1145/3689942.3694742.

Telecommunications and Digital Government Regulation Authority. 2026. "Initiatives - TDRA." Tdra.Gov.Ae. 2026. https://tdra.gov.ae/en/About/initiatives.

———. n.d. "Vision, Mission & Values - TDRA." Tdra.Gov.Ae. https://tdra.gov.ae/en/about/strategy.

The Business Year Editorial. 2026. "How Saudi Arabia Is Transforming Healthcare With AI." The Business Year. The Business Year. September 29, 2026. https://thebusinessyear.com/article/how-saudi-arabia-is-transforming-healthcare-with-ai-2026/?srsltid=AU7gw4U-PKdIc6IHM0BTm2iNZjGC6g52TgNbSIdMUnIz7NthLGoH4j8P.

The News Team. 2025. "Saudi Arabia's Healthcare Sector's Digital Transformation Comes after Cyber Threats Increase." Security Middle East Magazine. December 11, 2025. https://securitymiddleeastmag.com/cybersecurity/saudi-arabias-healthcare-sectors-digital-transformation-comes-after-cyber-threats-increase/.

Tulchinsky, Theodore H. and Elena A. Varavikova. (2014). Chapter 3: Measuring, Monitoring, and Evaluating the Health of a Population. The New Public Health (3rd eds.). Academic Press, 91–147. https://doi.org/10.1016/B978-0-12-415766-8.00003-3.

U.S. Food and Drug Administration. "Medical Device Cybersecurity: What You Need to Know." February, 4, 2022. https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know

U.S. Food and Drug Administration. "Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff." December 28, 2016. https://www.fda.gov/media/95862/download

U.S. Government Accountability Office (GAO). "Human Genomic Data: HHS Could Better Track Use of Foreign Testing Entities and Strengthen Oversight of Security Measures." April 30, 2025. https://www.gao.gov/assets/gao-25-107377.pdf

Wakili, Abubakar, et al. (2025). A digital twin-enhanced cybersecurity framework for IoT in healthcare: Applications in industry 4.0. Telematics and Informatics Reports,20. https://doi.org/10.1016/j.teler.2025.100254.

World Health Organization (WHO). "Cyber-attacks on Critical Health Infrastructure". February 6, 2024. https://www.who.int/news-room/questions-and-answers/item/cyber-attacks-on-critical-health-infrastructure

World Health Organization (WHO). (2024). "Guidance for human genome data collection, access, use and sharing." https://iris.who.int/server/api/core/bitstreams/c32ba78e-de45-416a-a5ae-3863b93e4628/content

World Health Organization (WHO). (2023). "Regulatory considerations on artificial intelligence for health." https://iris.who.int/server/api/core/bitstreams/ad62580f-540f-4e36-b957-e7f2946ae1fb/content

World Health Organization (WHO). WHO Director-General's remarks at Meeting of the UN Security Council on threats posed by ransomware attacks against hospitals and other health-care facilites and services. November 8, 2024. https://www.who.int/news-room/speeches/item/who-director-general-s-remarks-at-meeting-of-the-un-security-council-on-threats-posed-by-ransomware-attacks