universität Witten/Herdecke

Cybersecurity

All Hands on Deck in a World of connected Healthcare



www.atlasdigihealth.org

Table of Contents

Table of Contents 1
Preface 2
Executive Summary 3
1. Cyberattacks are an increasing threat 5
2. Data exchange and connectivity of hospital systems is rising 7
  2.1. Architecture of a connected healthcare system 8
  2.2. IT applications for patient treatment 10
3. Cybersecurity is everyone's job 13
4. Leadership defines the cybersecurity culture of a hospital 19
5. Cybersecurity threats in the hospital context 21
6. How can cybersecurity measures be aligned? 24
7. Conclusion 27
References 29
Acknowledgements 33
The ATLAS Project 34

Preface

Healthcare systems have become increasingly interconnected. The adoption of technologies such as electronic health records, artificial intelligence, and the Internet of Things (IoT) has brought significant advantages to patient care. These advancements streamline administrative processes, enable more efficient treatment workflows, and even help in diagnosis. However, this digital transformation also introduces new vulnerabilities. Hospitals have become prime targets for cybercriminals, with rising incidences of data breaches and system disruptions.

In this whitepaper we examine the complex system architecture of hospitals, illustrating how various technological components interact to support patient treatment. We highlight the critical role of cybersecurity within this infrastructure, emphasizing that a hospital's cybersecurity requires a holistic approach that aligns human behavior, technological solutions, and organizational practices.

The involvement of key cybersecurity actors ranging from IT professionals to clinicians and administrative staff is essential in building a resilient cybersecurity framework. By understanding the specific needs and challenges of each group and by fostering a cybersecurity culture, hospitals can develop tailored strategies that enhance security without disrupting daily operations.

The insights provided in this whitepaper are designed to guide healthcare leaders in addressing the growing cybersecurity threats their organizations face. It offers practical approaches for integrating cybersecurity into hospital operations while maintaining a focus on patient care, operational efficiency, and compliance with regulatory standards.

We want to take this opportunity to thank our partners in business and academia for the valuable collaboration, and the state of North Rhine-Westphalia, especially the Ministry of Economic Affairs, Industry, Climate Action and Energy, for financial grants to the ATLAS project.

Witten, October 2024

Executive Summary

As healthcare systems become increasingly interconnected, the importance of cybersecurity in the healthcare industry has grown substantially.
Approximately 30% of the world's processed data volume originates from the healthcare industry. The digitalization of the sector helps to improve patient treatment, for example, in terms of decision support. Meanwhile healthcare data is considered highly valuable on the black market, which has led to the healthcare sector (especially the hospital sector) becoming a primary target for cybercriminals.

Hospital systems are composed of a multi-layered system architecture, with various applications used throughout patient's hospital stay.
This multi-layered architecture includes various devices within the Internet of Things (IoT). Patient data can be directly traced from medical devices, processed and analyzed within the hospital network, and later displayed in the different IT applications that are part of the Hospital Information System (HIS). The process is not limited to internal use; a hospital is able to share patient data with other healthcare organizations or with the patients themselves through Health Information Exchanges (HIEs).

Within a hospital different actors, having varying motivation and education in terms of cybersecurity are involved.
Cybersecurity influences different groups within the hospital, not only the IT department. Depending on their position cybersecurity actors may have varying degrees of motivation and education in the field. Understanding their perspective on cybersecurity and the challenges they face in conjunction with it, helps in the development of cybersecurity concepts and gives insight in potential threats.

The hospital's leadership sets the tone for the cybersecurity strategy and culture.
Leadership is responsible for meeting regulatory cybersecurity requirements and adapting these requirements to hospital processes. On the one hand, streamlined processes for effective patient care are essential, while on the other hand, cybersecurity risks must be minimized by implementing protective measures. It is the leadership's role to balance these aspects, provide sufficient resources and a clear cybersecurity strategy.

Cybersecurity threats are diverse but increasingly focus on exploiting the human factor.

Hospital staff often works under high pressure, with patient treatment being the main focus. Cybercriminals exploit this by using tactics such as phishing attempts combined with precise social engineering. It becomes clear that robust cybersecurity cannot be achieved solely through advanced technological infrastructure, but through cybersecurity concepts that consider the interaction between human, technology, and organization.

A joint development of cybersecurity measures in conjunction with a shift in culture improve a hospital's future cyber readiness.

Introducing a proactive and inclusive cybersecurity approach, combined with targeted communication and training concepts, will improve the acceptance and effectiveness of cybersecurity measures. A hospital that adopts this approach will not only defend against cyber-threats but also position itself as a leader in the secure delivery of modern healthcare.



1. Cyberattacks are an increasing threat

Cyberthreats are an increasing risk across all sectors, resulting in an economic damage of approximately 206 billion Euro in Germany in 2023. Contributing factors included reputational damage; failure, theft or damage to information and production systems; legal disputes; investigations and replacement measures, and blackmail with stolen data or encrypted data (1).

The rapid digitalization of the healthcare sector, combined with the growing volume and exchange of electronic patient data, has made healthcare one of the most targeted industries for cybercriminals. In 2023, around 30% of the world's processed data comes from the healthcare industry. By 2025, the volume of healthcare data is projected to increase by 36% compared to 2020. This surge is largely driven by advancements in imaging technologies, such as video diagnostics, and the expanded adoption of electronic health records within hospitals (2).

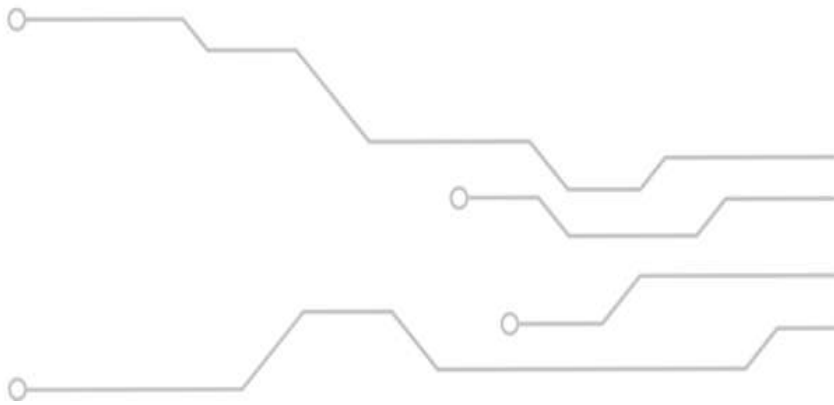
In Europe, 53% of cyber incidents occurred at healthcare providers, with hospitals being the primary target (42% of the attacks on healthcare providers) between January 2021 and March 2023 (3). According to the Federal Office for Information Security in Germany, the risk of cyberattacks on hospitals has reached an all-time high (4).

Healthcare data is considered even more valuable than credit card data because it contains sensitive information such as names, social security numbers, dates of birth, protected health information (PHI), and, depending on the region, also patients' credit card information (5).

In the context of the healthcare industry, cybersecurity attacks not only present a financial risk but also have the potential to disrupt patient care. For instance, test results and radiological images may become inaccessible, or critical examinations may be delayed or unable to be scheduled (6).

Due to the heightened risk of cybersecurity incidents in the healthcare industry, various legislative measures for cybersecurity and data protection have been introduced. Notable examples include the General Data Protection Regulation (GDPR) and the Cybersecurity Act (CSA) in the European Union (7), along with HIPAA (Health Insurance Portability and Accountability Act) in the USA. Non-compliance with these regulations can result in significant financial penalties (8).

Given these facts, it is important for healthcare leaders to understand which factors influence their cybersecurity posture, how healthcare systems are structured, and how cybersecurity measures can be effectively aligned through the integration of human, technology, and organization (HTO). Cybersecurity encompasses both technological and non-technological measures taken to protect an organization's IT related assets (9).



2. Data exchange and connectivity of hospital systems is rising

The amount of data processed and shared by hospitals is rising, both internally and externally. This is reflected in the increasing use of health information exchange (HIE) (10). Figure 1 illustrates a health information exchange where a central organization manages the data, though other types of health information exchanges also exist (11, 12). HIE is used across different countries globally, including Germany and the Unites States (13, 14).

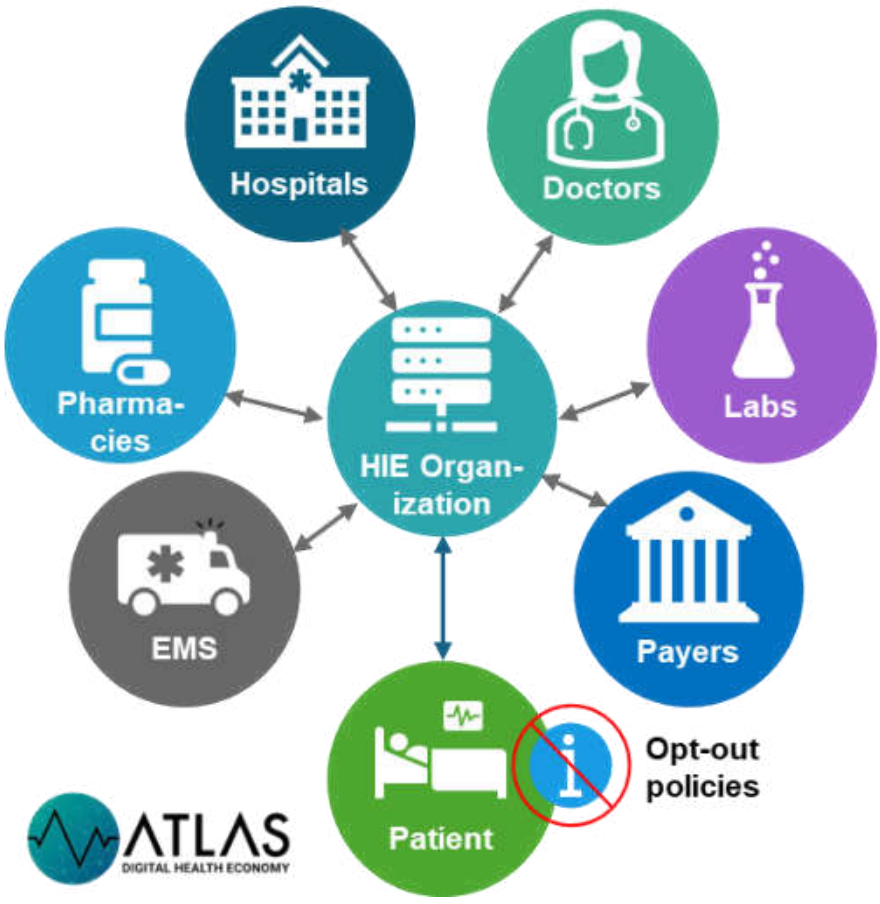


Figure 1: Structure of Health Information Exchange (HIE)

As hospitals are a primary target for cybercriminals, a multi-layered system architecture is applied, to enhance data security both internally and externally.

2.1. Architecture of a connected healthcare system

Figure 2 provides an overview of the system architecture, of a connected healthcare system in a hospital. A highly modular system supports the effective adoption of cybersecurity technologies (9). The depicted system architecture consists of four distinct layers.

In the first layer healthcare data is collected through various devices and sensors. Healthcare data is encoded using data standards, for example HL7 (15). In the second layer healthcare data is analyzed, processed, filtered, and then stored within the hospital network. At this point it is possible to access the data from different devices within the network, but also through network APIs from other healthcare institutions or different third-parties. To ensure the security, integrity and confidentiality of the data, standardized network protocols like TCP/IP are used for data transmission (15).

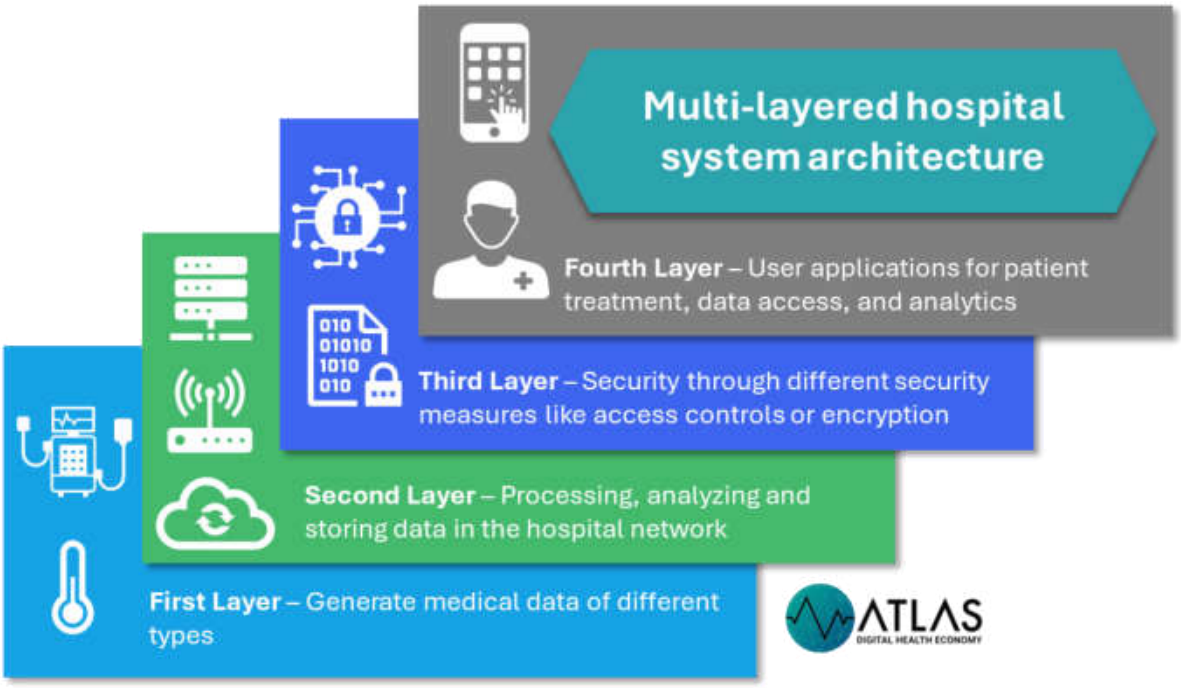


Figure 2: Architecture of a connected healthcare system (15)

The third layer is dedicated to securing the hospital system through various integrated security measures. For example, cybersecurity efforts concentrate on user authentication and user privileges (15). With multifactor authentication, users must not only enter their password but also verify their identity using dynamic authentication codes displayed on a security token or smartphone. Once access to the system is granted, users should only be able to view and modify information pertinent to their role, in accordance with the principle of least privilege (16).

Another security measure is data encryption both when data is stored (data at rest) and during transmission. A commonly used encryption method for healthcare data is the Advanced Encryption Standard (AES) (15).

Additional security can be achieved through the implementation of a robust firewall and the use of intrusion detection and intrusion prevention systems. An intrusion detection system (IDS) passively identifies cyberthreats and alerts IT professionals, while an intrusion prevention system (IPS) can actively disrupt data flows and block network traffic from specific sources. Similar to the IDS, the IPS also informs IT professionals when cyberthreats are detected. (17).

The applications utilized by users are located in the fourth layer. These applications allow users, such as clinicians, to access patient data via clinical workstations or portable devices. With the advent of emerging tools like big data and artificial intelligence, analytical procedures are also performed at this layer, aiming to assist clinicians with treatment decisions, visualize data, and optimize processes based on the patient data within the system (15).



2.2. IT applications for patient treatment

During a hospital stay, a patient transitions through various phases, each involving the use of healthcare-related IT applications located in the fourth system layer. In this whitepaper, we have categorized these phases into admission, diagnosis, therapy, and discharge. Throughout these phases, a complex ecosystem of applications is utilized to process patient data (see Figure 3). In the following chapter, we will provide a comprehensive overview of the application structure within a hospital.

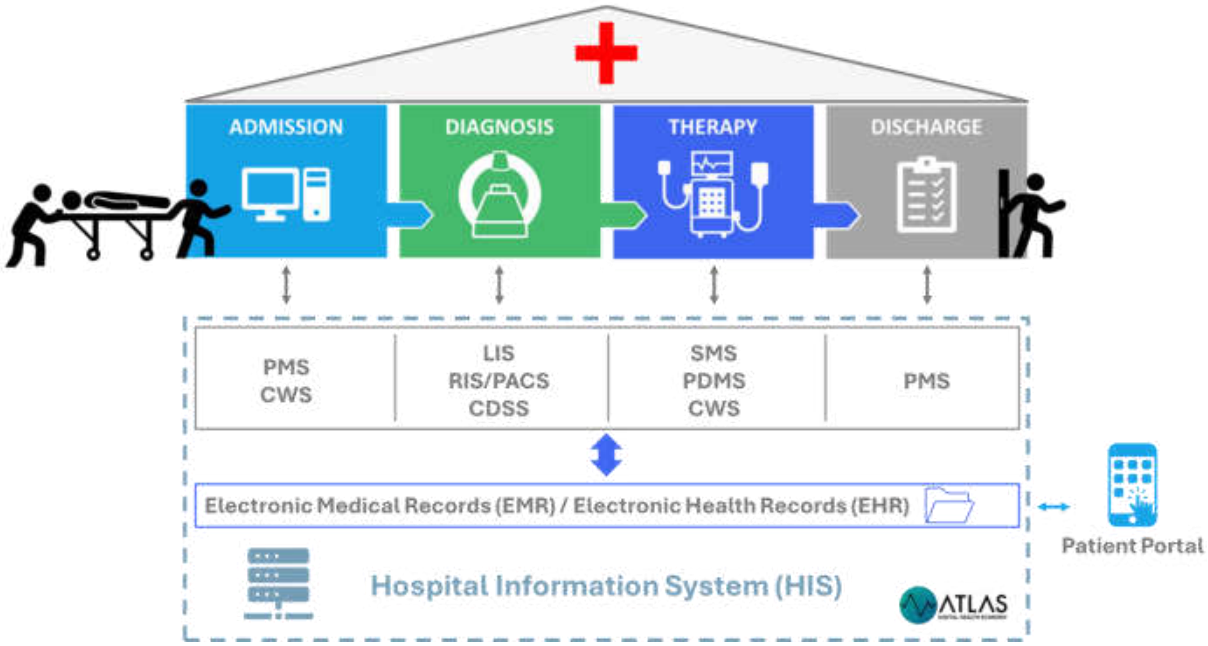


Figure 3: Patient journey through hospital system applications

When the patient is admitted to the hospital, their data is entered into the Practice Management System (PMS). Administrative hospital staff enters patient master data either manually or via an electronic health card into the PMS. The PMS is primarily used for administrative tasks such as patient admission, billing, insurance claims, scheduling appointments, or relocating patients within the hospital (18).

Once the patient data is entered into the Practice Management System (PMS), it becomes accessible to healthcare professionals through the Clinical Workplace System (CWS). The CWS is used by healthcare professionals to access patient information throughout their workday. It contains essential data, including details on diagnosis and treatment, and is therefore utilized frequently during the patient's hospital stay. Based on the patient's data, healthcare professionals can formulate an initial diagnosis (19).

During the diagnosis phase, different tests and radiology screenings of the patient may be performed. To facilitate this, various subsystems are accessed by healthcare professionals. For example, a Laboratory Information System (LIS) is used for scheduling laboratory tests at external laboratories and for exchanging specific test results. At the same time, the LIS may, for example, suggest appropriate tests based on the patient's data (20). Similarly, the Radiology Information System (RIS) is used for scheduling radiological examinations for patients, but also offers additional functions, such as decision support, displaying dashboards, or populating patient data (21). Results of radiological interventions are stored in a proprietary data format and can be accessed through the Picture Archiving and Communication System (PACS). Within the PACS, patient information can be shared between different clinicians (22).

As already presented, the LIS and the RIS can help with the diagnosis of the patient. Additionally, Clinical Decision Support Systems (CDSS) can be used in forming a diagnosis. Based on the patient's data and current scientific evidence, these systems are able to provide evidence-based treatment recommendations (23).

When the clinicians have decided on a patient therapy, different systems are utilized. Examples are Surgery Management Systems (SMS), which are used for scheduling the surgery and planning the surgery itself. Within these systems it can be defined which materials will be needed and how the surgery is going to be performed. During the surgery, critical patient data is documented in the system. These systems can also assist surgeons in determining the next steps during the procedure. Documenting the surgery in the system not only helps to retrace the procedure and the materials used in the future but also aids in reimbursing the cost of the surgery (24, 25).

During the therapy phase, a Patient Data Management System (PDMS) can be used, particularly in intensive care. With the PDMS, real-time patient data is monitored and tracked, and based on that data, decision support can be provided. Decision support may include identifying contraindications or assisting in dosage calculation (26).

At the time of patient discharge, the Practice Management System (PMS) is used for billing based on the patient's treatment and for providing information for follow-up care (18).

Throughout the process, patient data is stored in an electronic file. There are two different types of files for storing patient data electronically: the Electronic Medical Record (EMR) and the Electronic Health Record (EHR). The EMR stores patient data electronically within a single healthcare organization, while the EHR can be maintained and accessed by multiple institutions, such as other hospitals, health insurers, or local physicians, allowing healthcare organizations to access the patient's medical history (27).

Patients can also access their data stored in the EHR via an electronic patient portal. Through this portal, they, for example, have access to visit summaries, test results, and allergy information, and can securely exchange information with healthcare providers, as well as schedule appointments, such as teleconsultations (28).

The applications presented are part of the Hospital Information System (HIS). As such, the HIS is used across various departments within a hospital (for example, administration, radiology, or surgery). The HIS configuration may vary based on the different subsystems a hospital has implemented and the specific requirements of the hospital staff (29).

3. Cybersecurity is everyone's job

There are several cybersecurity actors within the hospital environment (see *Table 1*). To understand their motivation and work in more detail, the following section illustrates how these actors are affected by cybersecurity.

Table 1: Characterization of cybersecurity actors in the hospital



Nurses

Users of healthcare technology, administrative technology, and private devices

Motivation

"My main motivation is delivering excellent patient care. I need efficient access to patient data and often manage multiple patients simultaneously. While protecting sensitive information is crucial, cybersecurity measures must secure data without impeding my workflow or slowing me down. Balancing security with efficiency is essential to ensure I can provide timely and effective care."

Education in Cybersecurity

Recurring trainings based on hospital cybersecurity programs



Physicians

Users of healthcare technology, administrative technology, and private devices

Motivation

"*I want to ensure my patients' safety and privacy by safeguarding their medical records from cyber threats. With many tasks at hand, I need robust cybersecurity that protects data without obstructting my ability to provide efficient and effective care.*"

Education in Cybersecurity

Recurring trainings based on hospital cybersecurity programs



Leadership/Management

Users of administrative technology, as well as private devices

Motivation

"*As a manager, I want processes to run smoothly and efficiently without interruptions. I am aware of the cyber risks that could lead to system outages or the loss of patient data. We need to be as effective and streamlined as possible, but we cannot afford system outages or penalties due to non-compliance with cybersecurity regulations.*"

Education in Cybersecurity

Recurring trainings based on hospital cybersecurity programs, plus further training in terms of liability in case of cybersecurity incidents



IT Professionals

Managing IT processes and IT security in the hospital, with access to all systems

Motivation

"*I want to safeguard patient data and ensure the security of our interconnected devices. By balanceing cybersecurity with seamless operation, I strive to protect sensitive information, maintain the trust of both patients and medical staff, and prevent disruptions to healthcare services.*"

Education in Cybersecurity

Expert in the field, preparing trainings for the other actors and defining the cybersecurity strategy together with management



Administrative Staff

Users of administrative technology, as well as private devices

Motivation

"*As administrative staff, I perform several roles: managing billing, admissions, discharges, and capacity planning. With extensive use of digital systems to streamline processes, I need cybersecurity measures that protect data while not interfering with my daily work, ensuring efficient and trustworthy services.*"

Education in Cybersecurity

Recurring trainings based on hospital cybersecurity programs



Patients

Users of private devices in the hospital network

Motivation

"*I want to recover as quickly as possible. During my hospital stay, I use my devices to stay in contact with my relatives. I trust the hospital to protect my data and provide the best possible treatment. After discharge, I want to access my health information at home and schedule appointments as easily as possible.*"

Education in Cybersecurity

Potential basic cybersecurity education



Visitors/Relatives

Users of private devices in the hospital network

Motivation

"As a visitor using personal devices on the hospital network, my motivation is to stay connected during visits. I need reliable access to the internet for communication and information, without interruptions, so I can remain in touch and informed while performing my duties or visiting my relatives. Additionally, I want to communicate with my relatives and potentially with medical staff when I am not in the hospital."

Education in Cybersecurity

Potential basic cybersecurity education

Nurses are the largest group of healthcare professionals in Germany. In 2022, 29% of healthcare workers in Germany were nurses (30). The widespread use of electronic health systems poses challenges for them (31). However, in many counties, there is still a lack of regulations demanding cybersecurity training as part of the nursing curriculum (31). Nurses are frontline workers in the healthcare industry and therefore must use technologies safely and efficiently (31). Although nurses don't need to understand the complex code behind the systems, in the context of cybersecurity, they must follow certain basic cybersecurity principles. For example, they should store portable devices and records appropriately, avoid sharing passwords and change them frequently, refrain from clicking on suspicious links, notify IT in case of suspicious events, comply with hospital policies, and update the used devices (31). During their work, nurses often interact with the Clinical Workplace System (CWS) to retrieve patient information, such as prescribed medication.

Like nurses, physicians are also frontline healthcare workers. They process similar patient data in various systems (for example, test results, or images of radiological interventions) and therefore require the same fundamental cybersecurity education. Even though physicians have a senior title, studies have shown that they have lower cybersecurity competence scores than nurses and administrative staff. One possible explanation for this could be that physicians have even more demanding cognitive tasks than other staff in hospitals, making cybersecurity less of a main priority (32).

With physicians working more and more with connected devices, understanding cybersecurity principles to ensure patient safety and to have adequate support is becoming increasingly relevant. Surgeons, for example, could implant a state-of-the-art morphine pump without having the cybersecurity background to understand and control its wireless security protocols (33).

Physicians need to communicate with each other for patient treatment. One factor to be considered in terms of cybersecurity is the use of private mobile devices. Mobile devices enable physicians to quickly exchange information, seek consultation from more experienced staff, or access health records at different locations, even when they are not in the hospital. Mobile devices are also used as a quick research tool for assistance in diagnosis, information on specific drugs, or as a dosage calculator. (34) (35).

Hospital management doesn't have direct patient contact but is involved in several areas of cybersecurity. First of all, they have access to the hospital system and, therefore, need to follow basic cybersecurity procedures, as already described above. Their role in terms of cybersecurity is to establish sufficient policies, analyze cyber risks, and, based on that, provide sufficient resources to address cyber threats for the hospital accordingly (36).

IT professionals play a key role in a hospital's cybersecurity infrastructure. They have the highest education in the field of cybersecurity and work with both management/administration and clinicians. One issue to point out is that, even though IT departments have the highest knowledge in terms of cybersecurity, they are often understaffed and underfunded, leading to a lack of cybersecurity experts within the departments and, therefore, potential gaps in the hospital's cybersecurity infrastructure (37). IT departments in hospitals cover a wide range of tasks, they are responsible for designing the hospital's system environment, managing the IT hardware, and balancing the user requirements with cybersecurity needs in an area of very sensitive data. They have to update systems, inform management about developments in terms of cybersecurity, and train the other staff according to their tasks. IT professionals are the ones restoring systems in case of a cybersecurity incident and also coordinate the preventive measures in a hospital. Consequently, they are involved in all layers of the connected healthcare system (see Figure 2). The rising number of cyberattacks and the technological development of connected healthcare systems have led to a high demand for IT professionals in this field (37).

Administrative staff also handles patient data, for example, during patient administration and billing in the Practice Management System (PMS). They have to adhere to the same basic cybersecurity principles as the other actors in the hospital. Therefore, they receive regular cybersecurity training to be aware of cyber risks during their work. One factor to be considered for administrative staff and hospital management is work from home (potentially with their own devices with improper security measures) (38).

Looking at the hospital staff in general, recurring cybersecurity trainings have a positive effect on cybersecurity awareness. Personnel with more work experience and, therefore, more cybersecurity training tends to have a higher awareness in this field (32).

In contrast to hospital staff, it cannot be assumed that patients or visitors receive regular cybersecurity training in their lives. While patients and visitors do not have direct access to the hospital system, during their hospital stay, they are likely to use the hospital's wireless network. Without proper separation of hospital networks, devices used by patients or visitors could pose cybersecurity risks. Additionally, hospital staff may need to remotely communicate with relatives about the patient's health information. Furthermore, as shown in Figure 3, with the increasing use of electronic health records (EHR), patients can access their health data outside the hospital environment, which poses additional risks as they access those records with personal devices over potentially unsecured network connections (38).

4. Leadership defines the cybersecurity culture of a hospital

Cybersecurity is a synergy between people, procedures, and technology. Leadership is responsible for fostering a cybersecurity culture, managing third parties, and providing the resources and non-technical measures necessary to enhance cybersecurity (9).

Effective cybersecurity can improve an organization's reputation while simultaneously increasing its performance by establishing robust internal procedures and limiting the risk of data breaches (9).

Ultimately, leadership is also responsible for complying with cybersecurity legislation and, therefore, preventing financial penalties (8).

Understanding the factors that influence the adoption of cybersecurity measures, such as technological compatibility with the system, perceived usefulness, and ease of use (9), together with external factors like government regulations (8), helps leadership to allocate resources accordingly.

Direct accountability and sponsorship from top management regarding cybersecurity helps with the adoption and effectiveness of cybersecurity procedures, policies, and technologies (9). Therefore, a high-level management position specifically addressing cybersecurity topics and being responsible for cybersecurity, such as a Chief Information Security Officer (CISO), should be established (39).

Cybersecurity policies include a general cybersecurity policy, business continuity plans, disaster recovery plans, continuity of operations plans, as well as criticality assessments of IT processes. In their documentation, organizations should identify strategies on how to protect themselves against cyberattacks and how to continue operations, retrieve data, and restore systems in the event of a cybersecurity incident (40).

Leadership should also govern the hospital's risk management (8). Cyber risks should be identified proactively, involving different cybersecurity stakeholders in the risk management process (41).



Figure 4: Components of a Cybersecurity Strategy [7]

Threats to be identified include, for example, outdated software (38), third-party threats, data protection governance, asset management, maintenance, resource management, and compliance (40).

Finally, it is leadership's responsibility to establish a clear vision for the future of the organization's cybersecurity strategy by aligning technology with the individual attitudes of hospital staff (9). The strategy should raise awareness for the topic by using different communication methods, such as cybersecurity newsletters (42). Secondly, preventive measures, like routinely educating hospital staff within a framework of operational flexibility that allows hospitals to quickly adapt to new technologies and effectively respond to cyberattacks, should be established (9, 42). The third component of the strategy should be to implement a continuous lessons-learned approach. Cybersecurity events must be analyzed, and strategies adjusted accordingly. Periodic knowledge checks among hospital staff should also be conducted to set priorities in cybersecurity education, taking into account different education levels and varying motivations in terms of cybersecurity (see Figure 1).

5. Cybersecurity threats in the hospital context

The increased volume of exchanged data and the growing number of data exchange points bring many benefits to patient treatment (10). Digitalization enables hospitals to streamline administrative procedures, quickly gain insight into the medical history of patients upon arrival, and use digital tools for decision-making and diagnosis support.

At the same time, the connected health environment poses significant cybersecurity threats, making adequate risk management through cooperation between clinical, administrative, and information technology leaders essential (41).

In the following chapter, potential cyber threats to hospitals are outlined. Figure 5 provides an overview of cyberthreats in a connected healthcare system.

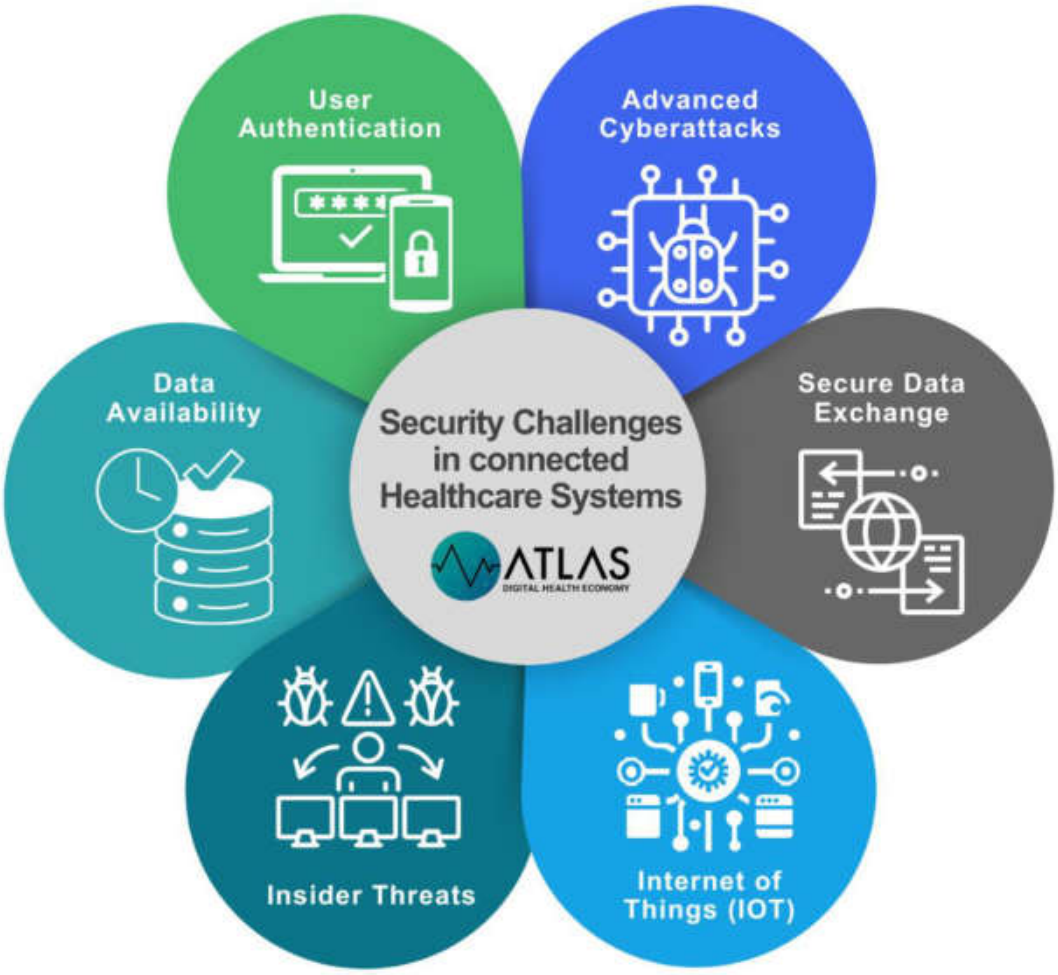


Figure 5: Security Challenges in connected Healthcare Systems (15)

One factor to consider is the Internet of Things (IoT), which consists of various connected devices, such as medical devices. The connection between medical devices offers multiple benefits for patient treatment, such as automated detection of patient parameters or electronic dose adjustments. While these benefits are evident, connecting medical devices to the hospital network introduces various technological challenges (e.g., interoperability of different devices and data storage) and security risks. In terms of security, due to the open communication structure and sometimes outdated software of medical devices, hackers could alter transmitted data or alert information (15).

Different types of cyberattacks can be categorized as advanced cyberattacks. Replay attacks, for example, involve intercepting and retransmitting data to manipulate the system. Denial of Service (DoS) attacks overwhelm systems with a large volume of traffic. Man-in-the-middle attacks involve data interception during communication between different devices or systems. Modifying data or software to compromise system integrity is classified as a modification attack.

System compromises intentionally or unintentionally caused by authorized personnel are called insider threats (15). Such insider threats could involve staff violating cybersecurity protocols by deleting, misusing, altering, or distributing data (31).

Threats such as remote work without appropriate authentication or an unsecured connection, as well as the use of personal devices within the hospital, have to be considered as well (38).

One growing threat is ransomware, which is malicious software that blocks access to IT systems and is often installed via phishing emails opened within the hospital network. To regain access to their systems, healthcare organizations typically need to pay a ransom to the cybercriminal (8).

Even though there is specialized training regarding on how to critically evaluate phishing emails, as much as 14.2% of phishing attempts are successful. Reasons include advanced targeting technologies or precise social engineering by the cybercriminals (43).

A lack of data availability, for example, caused by a ransomware attack, malfunctions in the system applications, or disruptions in the hospital's network connection (15), could lead to systems not functioning as planned, missing evidence for diagnosis and treatment decisions, or problems in administrative procedures like billing or locating patients (6).

When looking at cyberthreats, it can be stated that a significant amount of cybersecurity incidents are not caused by system weaknesses but by the human factor in cybersecurity. Risks include a lack of awareness, lack of knowledge of internal procedures, and difficulties integrating cybersecurity measures into daily work (44).

The risk that even well-trained staff will make unintentional cybersecurity errors increases when they are working under high pressure and without adequate resources.

Literature shows that high inpatient workloads (many acute care beds, high bed percentage used, and the severity of cases treated) greatly impact the risk of healthcare data breaches (8). A high inpatient workload can cause clinicians to bypass security measures and implement ad hoc workarounds due to the complex system environment and time pressure, thereby creating opportunities for data breaches (45).

As stated above, IT departments in hospitals often lack personnel focused on cybersecurity, requiring IT staff to cover many different tasks simultaneously, which can lead to potential weaknesses in the IT security infrastructure (37). The high demand for IT professionals makes adequate staffing challenging. IT departments are often underfunded, and hospitals compete against other industries that are often willing to pay higher salaries to IT professionals. This situation forces hospitals to rely on external support to respond to data breaches (37).

The diverse mix of cybersecurity actors within the hospital, highlights that it is challenging to find one-size-fits-all solutions in cybersecurity, so measures have to be developed in a broader context.



6. How can cybersecurity measures be aligned?

Cybersecurity of a hospital is a product of collaboration between human, technology, and organization (9). This collaboration is referred to as the HTO concept (46). In the context of cybersecurity, "human" refers to individuals in specific groups with distinct experiences and motivations, as reflected by the cybersecurity actors in Table 1. “Technology” encompasses the system architecture, the system applications, and the accompanying cybersecurity measures. Lastly, “organization” is represented by hospital policies, the culture toward cybersecurity, and the cybersecurity strategy governed by management (47). Outside this concept, there are environmental factors influencing the interaction between human, technology and organization, such as external service providers or legislation (see Figure 6).



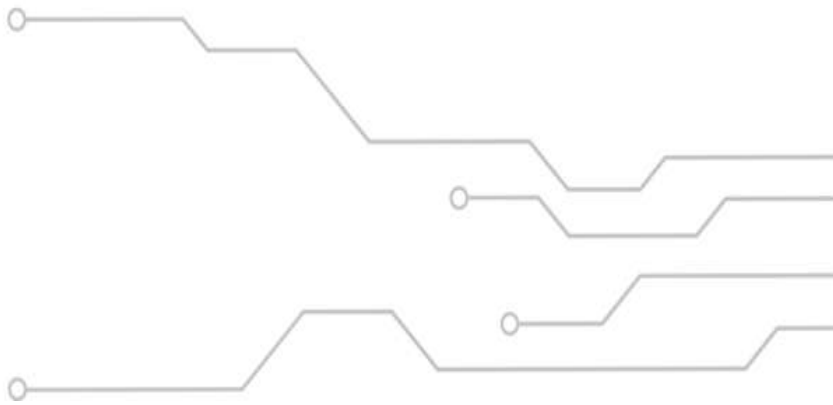
Figure 6: HTO concept in the hospital context

Given the fact that most cybersecurity incidents are associated with the human factor (32, 38), it can be stated that both technological and organizational measures for preventing cybersecurity incidents have to be aligned with the cybersecurity actors, as the conditions for the work in the area of cybersecurity are mediated by technology and organization (47).

For aligning human with organization and technology, training is essential. Cybersecurity training has been an active area of investigation for the past several years, even beyond the scope of the healthcare industry (39). Since the human factor is a key influence on cyber incidents, well-planned and tailored training concepts are needed. Trainings should be held regularly and cover best practices, for example in identifying phishing attempts, setting secure passwords, or how to handle data. They should also address the IoT as a potential source of cyberattacks (15).

To achieve greater success, trainings should be structured based on the audience's technical proficiency and the cybersecurity tasks they perform in their daily work (41). These trainings should demonstrate the added security value in terms of patient safety and operational continuity, as cybersecurity measures can sometimes be perceived as disruptive to the work of system users.

The human factor should also be considered in the development of security measures. These measures should be developed with shared ownership, addressing both security concerns and a user-centric design (41). The different cybersecurity actors have deep insights into their individual tasks and, therefore, are able to highlight challenges related to cybersecurity measures. Clinicians, for example, have direct patient contact and should be involved in the development. They can highlight which measures could be integrated into a streamlined workflow and which measures would create additional workstreams, potentially compromising the time available for patient treatment (25).



One example to consider in the development of cybersecurity measures is the use of private personal devices by clinicians. In a joint development of cybersecurity measures, clinicians could highlight that they often have to use their personal electronic devices to quickly exchange patient information with each other or conduct quick research tasks for diagnosis because no alternatives are provided by the hospital (34). Raising this issue during the development of cybersecurity measures could lead to the joint development of solutions, such as providing corporate mobile devices that allow clinicians to communicate securely and access the internet from a protected environment. Another alternative would be to establish bring your own device (BYOD) policies combined with secure connection methods and data separation (35). The joint development of cybersecurity measures would increase acceptance among clinicians, as it would be clear that patient care was the primary focus while cybersecurity measures were being developed (48).

Management should embrace a shift in culture, encouraging users to see cybersecurity not as an obstacle to their work but as an enabler, because it protects vital patient data and ensures that processes can run effectively and safely [37]. This is especially important for clinicians, as cybersecurity training competes with clinical training, which, from the clinician's perspective, provides more immediate benefits to patient care [31]. Self-studies, work-based trainings, and training materials prepared by cybersecurity professionals are potential education methods for hospital staff (44).

Apart from providing sufficient education for staff and fostering a cybersecurity culture, management should allocate adequate resources to handle cybersecurity activities, including resources in top management, such as a Chief Information Security Officer (CISO), who is directly accountable for cybersecurity (39). Furthermore, departments should have defined roles for cybersecurity, with, for example, one dedicated person in the IT department, responsible for cybersecurity activities.

Aligning human, technological, and organizational factors, alongside clear communication and the involvement of different actors in cybersecurity, will lead to a higher cybersecurity standard and better acceptance of cybersecurity measures, while simultaneously addressing user, regulatory, and security concerns (41).

7. Conclusion

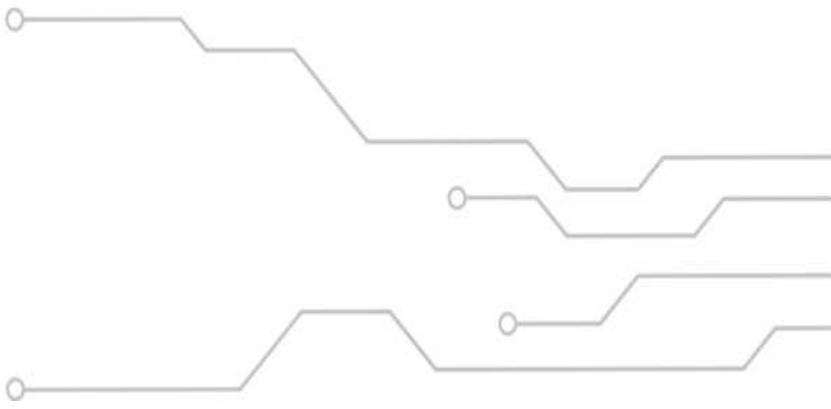
Cybersecurity is a topic gaining increasing importance in the healthcare industry as healthcare systems become more connected, with the healthcare sector, particularly hospitals, being the most frequently targeted by cybercriminals. A more connected healthcare industry offers various benefits for patient treatment, such as easier access to patient information, streamlined treatment processes, and assistance in diagnosis. However, this connectivity also introduces various cyberthreats, such as blocking system access through ransomware attacks, which pose significant risks to both patient treatment and overall workflows within the hospital.

This whitepaper introduced the complex system architecture of hospitals and how users interact with the hospital's applications. It becomes evident that cybersecurity is a product of the interaction between human, technology, and organization. Robust cybersecurity cannot be achieved solely through a complex security infrastructure. Management and IT professionals must involve the various cybersecurity actors within the hospital in the development of a sustainable cybersecurity concept.

With a joint approach to developing cybersecurity measures, there is an opportunity to view cybersecurity as an enabler for secure system operations and patient treatment, rather than as an obstacle to daily work.

Including the different cybersecurity actors in the hospital in the planning of cybersecurity measures will lead to a better understanding of the hospital's processes, including the needs and motivations of the different actors. Cyber risks will be more effectively identified, and mitigation strategies will be better aligned with the work of hospital staff, increasing acceptance of those measures. Additionally, future trainings can be tailored to the experience, motivation, and roles of the different actors within the hospital.

As the healthcare industry continues to evolve, the integration of emerging technologies, such as artificial intelligence and the Internet of Things (IoT), will further emphasize the need for adaptive and resilient cybersecurity strategies. By embracing a proactive and collaborative approach, hospitals can ensure that cybersecurity is not only a protective measure but also a key driver of innovation, patient safety, and operational excellence in the digital age. This will position healthcare organizations to not only defend against cyberthreats but also succeed in an increasingly connected and data-driven healthcare ecosystem.



References

1. Wintergerst R. Wirtschaftsschutz 2023. Berlin; 2023 [cited 2024 Jul 2]. Available from: URL: https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf.

2. Boehncke K, Duprac G, Sparey J, Valente A. Tapping Into New Potential: Realising the Value of Data in the Healthcare Sector 2023 [cited 2024 Aug 15]; (101). Available from: URL: https://www.lek.com/insights/hea/eu/ei/tapping-new-potential-realising-value-data-healthcare-sector.

3. Theocharidou M, Lella I, editors. ENISA threat landscape report: Health sector (January 2021 to March 2023). Heraklion: ENISA_2; 2023.

4. Bundesregierung. Drucksache 20/10907: Antwort der Bundesregierung auf die Kleine Anfrage der Frakton der CDU/CSU Drucksache 20/10757 [Cyberattacken auf Krankenhäuser - Sachstand und Handlungsbedarf]; 2024.

5. Frith KH. Data Breaches in Health Care: Preparing Students to Avoid Unsafe Practices. Nurs Educ Perspect 2019; 40(6):388–9.

6. Clarke R, Youngstein T. Cyberattack on Britain's National Health Service - A Wake-up Call for Modern Medicine. N Engl J Med 2017; 377(5):409–11.

7. Biasin E, Yaşar B, Kamenjašević E. New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act. Law Tech Hum 2023; 5(2):43–58.

8. Dolezel D, Beauvais B, Stigler Granados P, Fulton L, Kruse CS. Effects of Internal and External Factors on Hospital Data Breaches: Quantitative Study. J Med Internet Res 2023; 25:e51471.

9. Hasani T, O'Reilly N, Dehghantanha A, Rezania D, Levallet N. Evaluating the adoption of cybersecurity and its influence on organizational performance. SN Bus Econ 2023; 3(5):97.

10. Choi SJ, Chen M, Tan X. Assessing the impact of health information exchange on hospital data breach risk. Int J Med Inform 2023; 177:105149.

11. Akhlaq A, Sheikh A, Pagliari C. Defining Health Information Exchange: Scoping Review of Published Definitions. J Innov Health Inform 2017; 23(4):838.

12. Chen M, Esmaeilzadeh P. Adoption and use of various health information exchange methods for sending inside health information in US hospitals. Int J Med Inform 2023; 177:105156.

13. Payne TH, Lovis C, Gutteridge C, Pagliari C, Natarajan S, Yong C et al. Status of health information exchange: a comparison of six countries. J Glob Health 2019; 9(2):204279.

14. Holmgren AJ, Esdar M, Hüsers J, Coutinho-Almeida J. Health Information Exchange: Understanding the Policy Landscape and Future of Data Interoperability. Yearb Med Inform 2023; 32(1):184–94.

15. Singh J. Challenges with Medical Devices Connected To Hospital Network. IJRASET 2024; 12(6):735–49.

16. Bhukya CR, Thakur P, Mudhivarthi BR, Singh G. Cybersecurity in Internet of Medical Vehicles: State-of-the-Art Analysis, Research Challenges and Future Perspectives. Sensors (Basel) 2023; 23(19).

17. Luber S, Schmitz P. Was ist ein Intrusion Prevention System (IPS)?: Security Insider; 2017 [cited 2024 Aug 1]. Available from: URL: https://www.security-insider.de/was-ist-ein-intrusion-prevention-system-ips-a-612859/.

18. Bethany Nock. What Is a Medical Practice Management System?: Gebauer Company; 2017 [cited 2024 Jul 4]. Available from: URL: https://www.gebauer.com/blog/medical-practice-management-system.

19. Prokosch H-U. KAS KIS EKA EPA EGA E-Health: Ein Plädoyer gegen die babylonische Begriffsverwirrung in der Medizinischen Informatik 2001.

20. Sepulveda JL, Young DS. The ideal laboratory information system. Arch Pathol Lab Med 2013; 137(8):1129–40.

21. Nance JW, Meenan C, Nagy PG. The future of the radiology information system. AJR Am J Roentgenol 2013; 200(5):1064–70.

22. Eichelberg M, Kleber K, Kämmerer M. Cybersecurity in PACS and Medical Imaging: an Overview. J Digit Imaging 2020; 33(6):1527–42.

23. Toh Z an, Berg B, Han QYC, Hey HWD, Pikkarainen M, Grotle M et al. Clinical Decision Support System Used in Spinal Disorders: Scoping Review. J Med Internet Res 2024; 26:e53951.

24. Ulmeanu M-E, Mateș IM, Doicin C-V, Mitrică M, Chirteș VA, Ciobotaru G et al. Bespoke Implants for Cranial Reconstructions: Preoperative to Postoperative Surgery Management System. Bioengineering (Basel) 2023; 10(5).

25. Healthcare Digital. Was ist ein OP-Management-System? 2020 Aug 28 [cited 2024 Jul 12]. Available from: URL: https://www.healthcare-digital.de/was-ist-ein-op-management-system-a-81f31dbc91380dd6dc630be219da7983/?r=ext.

26. Rosenzweig C. PDMS (Patient Data Management System): What you should consider from a regulatory perspective. Johner Institute 2024 Apr 30 [cited 2024 Jul 12]. Available from: URL: https://blog.johner-institute.com/health-it/pdms-patient-data-management-system-what-you-should-consider-from-a-regulatory-perspective/.

27. Haan K, Main K. EHR Vs. EMR: What's The Difference? Forbes Advisor 2024 Jun 1 [cited 2024 Jul 12]. Available from: URL: https://www.forbes.com/advisor/business/software/ehr-vs-emr/.

28. Lyles CR, Nelson EC, Frampton S, Dykes PC, Cemballi AG, Sarkar U. Using Electronic Health Record Portals to Improve Patient Engagement: Research Priorities and Best Practices. Ann Intern Med 2020; 172(11 Suppl):S123-S129.

29. Ebnehoseini Z, Tabesh H, Deldar K, Mostafavi SM, Tara M. Determining the Hospital Information System (HIS) Success Rate: Development of a New Instrument and Case Study. Open Access Maced J Med Sci 2019; 7(9):1407–14.

30. Singer K, Fleischer N. Arbeitsmarktsituation im Pflegebereich: Berichte: Blickpunkt Arbeitsmarkt. Nürnberg: Bundesagentur für Arbeit; 2024 [cited 2024 Jul 23]. Available from: URL: https://statistik.arbeitsagentur.de/DE/Statischer-Content/Statistiken/Themen-im-Fokus/Berufe/Generische-Publikationen/Altenpflege.pdf?__blob=publicationFile&v=7.

31. Kamerer JL, McDermott D. Cybersecurity: Nurses on the Front Line of Prevention and Education. Journal of Nursing Regulation 2020; 10(4):48–53.

32. Alhuwail D, Al-Jafar E, Abdulsalam Y, AlDuaij S. Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities. Appl Clin Inform 2021; 12(4):924–32.

33. Dr.A.Shaji George, A.S.Hovan George. Safeguarding the Cyborg: The Emerging Role of Cybersecurity Doctors in Protecting Human-Implantable Devices 2023.

34. Kraushaar J, Bohnet-Joschko S. Prevalence and patterns of mobile device usage among physicians in clinical practice: A systematic review. Health Informatics J 2023; 29(2):14604582231169296.

35. Wani TA, Mendoza A, Gray K. Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature. JMIR Mhealth Uhealth 2020; 8(6):e18175.

36. Busdicker M, Upendra P. The Role of Healthcare Technology Management in Facilitating Medical Device Cybersecurity. Biomed Instrum Technol 2017; 51(s6):19–25.

37. Wasserman L, Wasserman Y. Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Front Digit Health 2022; 4:862221.

38. Cartwright AJ. The elephant in the room: cybersecurity in healthcare. J Clin Monit Comput 2023; 37(5):1123–32.

39. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E et al. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors (Basel) 2021; 21(15).

40. Secure Controls Framework. Secure Controls Framework 2024_2. In: [cited 2024 Jul 22]. Available from: URL: https://securecontrolsframework.com/scf-download/.

41. Clarke M, Martin K. Managing cybersecurity risk in healthcare settings. Healthc Manage Forum 2024; 37(1):17–20.

42. Hartland M. The 123 of Cyber Security for Healthcare Organizations; 2018. Available from: URL: https://www.snapcomms.com/blog/the-123-of-cyber-security-for-healthcare-organizations.

43. Jalali MS, Bruckes M, Westmattelmann D, Schewe G. Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. J Med Internet Res 2020; 22(1):e16775.

44. Argyridou E, Nifakos S, Laoudias C, Panda S, Panaousis E, Chandramouli K et al. Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study. J Med Internet Res 2023; 25:e41294.

45. Choi SJ, Johnson ME. Do Hospital Data Breaches Reduce Patient Care Quality?; 2019.

46. Karltun A, Karltun J, Berglund M, Eklund J. HTO - A complementary ergonomics approach. Appl Ergon 2017; 59(Pt A):182–90.

47. Berglung M, Karltun A, Eklund J, Karintaus J. HTO – A Concept of Humans, Technology and Organisation in Interaction 2020 [cited 2024 Aug 2]. Available from: URL: https://www.diva-portal.org/smash/get/diva2:1502551/FULLTEXT01.pdf.

48. Weber M, Hacker J, Karintaus L, Pekkola S, vom Brocke J. PREPARING FOR CYBERATTACKS: A CASE STUDY OF RESILIENCE IN THE HEALTH-CARE SECTOR: Association for Information Systems; 2023 [cited 2024 Aug 2]. Available from: URL: https://aisel.aisnet.org/ecis2023_rp/314/.

Acknowledgements

This whitepaper is brought to you by the ATLAS team:

Prof. Dr. Sabine Bohnet-Joschko
Grigori Rogge
Hendrik Bensch
Björn Gostmann
Dr. Katharina Loboiko
Jan-Patrik Novoa Lill
Lara Schmidt
Mia Yang
Charlotte Peter

Please cite:
Rogge, G; Bohnet-Joschko, S (2024), Cybersecurity: All Hands on Deck in a World of Connected Healthcare. Whitepaper. ATLAS Innovation and Digitalization in Health- care, Witten/Herdecke University, Witten.

The ATLAS Project

The project "Innovation and Digital Transformation in Healthcare" (ATLAS-ITG), funded by the state of North Rhine-Westphalia through the Ministry of Economic Affairs, Industry, Climate Action and Energy, offers science-based solutions for practical challenges in the digital transformation of the healthcare sector.

The ATLAS (www. atlasdigihealth.org) conducts socio-scientific analyses on the impact of digitalization in the healthcare sector, connects flagship projects in North Rhine-Westphalia, and supports the theory-to-practice transfer by providing concise summaries of current studies and contextualizing technical innovations with use cases for health professionals.

Funded by the state of North Rhine-Westphalia



The ATLAS project is situated at the Chair for Management and Innovation in Healthcare at the Faculty of Management, Economics and Society at Witten/ Herdecke University. The chair team works on economic issues in and between organizations of the healthcare industry. The chair is a member of the Interdisciplinary Center for Health Services Research (IZVF) and contributes to the description, explanation, testing and evaluation of concepts that ensure high-quality healthcare.

More about the chair: www.uni-wh.de/MIG

More about Witten/Herdecke University: www.uni-wh.de

