Issues in Information Systems
Volume 23, Issue 1, pp 102-116, 2022

DOI: https://doi.org/10.48009/1_iis_2022_108

Cybersecurity as a unifying factor for privacy, compliance and trust: The Haga Hospital case

Angelica Marotta, *MIT, amarotta@mit.edu*
Stuart Madnick, *MIT, smadnick@mit.edu*

Abstract

Compliance and cybersecurity are crucial to many healthcare organizations. However, their implementation is often challenging, especially when privacy and trust are involved. An example is the case of the Haga Hospital in The Netherlands that was found in breach of the GDPR (General Data Protection Regulation) for inadequately protecting medical records. Failing to implement security controls prevented the organization from guaranteeing privacy protection and maintaining patient trust. Through the examination of this case and a brief comparison with a similar incident in Portugal, the paper investigated the context and the conditions associated with this breach and why they are closely related to privacy and trust. The results of this analysis suggest that cybersecurity can be considered a "unifying factor" between privacy and trust in the context of regulatory compliance. Thus, this study can be used by regulatory authorities and healthcare organizations to establish more focused cybersecurity measures and ensure a balance between compliance, security, and privacy.

Keywords: Cybersecurity, Compliance, Trust, Privacy, Healthcare

Introduction

In today's digital world, regulatory compliance in healthcare involves higher risks than those occurring in other industries. Due to their sensitive nature, healthcare data represent a tempting target for cybercriminals. Therefore, the industry has a unique responsibility to protect its cybersecurity infrastructure and address new vulnerabilities. To tackle this problem, laws have also been updated to establish standards for cybersecurity in medical environments. However, healthcare organizations face multiple challenges for managing security controls and meeting compliance requirements (Marotta & Madnick, 2021b). Moreover, in addition to the complexity deriving from security and compliance tasks, there are two other interrelated but distinct factors complicating cybersecurity efforts in healthcare: privacy and trust.

- **Privacy**. Privacy involves safeguarding personally identifiable information (PII) (Isaak & Hanna, 2018). The relationship between privacy and cybersecurity is critical because it can influence the quality of care. By definition, PII should be private, but it also falls under the security radar. On the one hand, personal information should be managed in a way that ensures appropriate usage by the people (i.e., doctors) who need to use that information. However, personal data should also be securely protected.

- **Trust**. While privacy and security risks can be addressed, they cannot be eliminated completely. As a result, patients need to have trust that their data are being kept private and secure in the best way possible (Iott et al., 2019). Trust also involves confidence that healthcare providers have appropriate supporting infrastructure and governance to comply with the high number of compliance requirements (Gerke et al., 2020).

Recently, healthcare providers and regulators have been confronted with significant data privacy and security issues, which have affected their operational and legal contexts as well as patient confidence.

An example is the case of the Haga Hospital in the Netherlands that was found in breach of the General Data Protection Regulation (GDPR) for inadequately protecting medical records (Herman Zaalberg, 2018). Failing to implement security controls prevented the organization from guaranteeing privacy protection and maintaining patient trust. This paper provides an in-depth analysis of the case and its implications.

Methodology and Study Design

We conducted this research with a combined methodology. The first method involved investigating the case of the Haga Hospital using qualitative *content analysis* of public sources. This approach helped extract and summarize critical information about the data breach, such as root causes, stakeholders, etc. The second method employed *narrative analysis* to describe the relevant events leading to the compliance failure and show the main issues arising from the case. The paper is organized as follows. First, it reviews the relevant research literature concerning security, privacy, and trust in healthcare compliance. Second, it investigates the context and the security issues associated with the breach that affected the Dutch hospital and why they are closely related to privacy and trust. Finally, this work compares case results with a similar incident in Portugal and examines the key lessons learned from analyzing the two GDPR violations.

Background and Literature Review

The relevant literature is highly dominated by research on the technical elements of cybersecurity in healthcare (Argaw et al., 2020; Martin et al., 2017). For example, Coventry and Branley (2018) discussed concerns relating to the security of healthcare data and devices. Similarly, Ayala (2016) addressed cyber-physical attacks against healthcare facilities and equipment. The same considerations apply to research on privacy and trust in healthcare. For instance, Iott et al. (2019) examined patients' privacy concerns and discussed the need to address several aspects of trust for patient behavior around information sharing with health care providers. In addition, other authors conducted specific empirical studies on cybersecurity compliance in healthcare; Yuan and Li (2019) investigated the GDPR's policy impact on the financial performance of hospitals across the European Union. Fan et al. (2020) examined privacy protection and GDPR compliance in mobile health applications.

Some authors also analyzed the relationship between privacy, security, and trust in healthcare. For example, Vaiyapuri et al. (2021) investigated security, privacy, and trust in the Internet of Medical Things (IoMT)-Enabled Smart Healthcare System.

However, while there is a growing body of literature concerning the relationship between security, privacy, and trust in healthcare operations, research on this topic is limited in the specific context of healthcare compliance. One of the closest studies related to this topic is the one performed by Cellier and Ghernaouti (2019). The authors identified the critical success factors of cybersecurity for e-health. They demonstrated that the effectiveness of cybersecurity depends on a combination of organizational, managerial, human, legal, and technical measures. Thus, after a careful examination of the literature on the subject, one of the most evident observations is that there is a very fragmented approach to investigating security, privacy, and trust in healthcare compliance. In particular, the majority of papers fall under three distinct research trends:

Cybersecurity and Healthcare Compliance

The majority of papers on cybersecurity and healthcare compliance focus on the critical compliance issues that the healthcare industry faces when complying with healthcare cybersecurity regulations. For example, some authors (Abraham et al., 2019; Mohammed, 2017) evaluated the current US compliance and regulatory

landscape of the healthcare industry concerning cybersecurity. They mainly focused on the fact that the healthcare industry fails to use tools and programs to ensure that information is secure and protected.

Some papers covered the topic, starting from an analysis of regulations. For example, some authors (Jackson & Rahman, 2019; Strielkina et al., 2018) investigated the problem by evaluating international regulations on medical and healthcare cybersecurity with particular reference to Internet of Things (IoT)-based systems. Conversely, others (Daniels & Bhatia, 2020) began their analysis by looking at reported incidents to examine modifications to legislation in healthcare.

Another nuance found in the literature also involves a more specific organizational perspective of the topic. For example, Parker (2020) focused on the main programs that healthcare organizations need to put in place to protect themselves against cybersecurity attacks and remain compliant.

Privacy and Cybersecurity in Healthcare Compliance

A significant body of research has examined the perception of security concerns in healthcare compliance from the viewpoint of privacy (Iyengar et al., 2018; A. C. Johnston & Warkentin, 2008; Nazir et al., 2019). For example, Breaux and Antón (Breaux & Antón, 2008) examined how efficient software systems' security and privacy requirements must be in order be appropriately aligned with relevant healthcare regulations. In another study, Bhuyan et al. (SS et al., 2020) provided recommendations for policymakers and healthcare organizations to strengthen cybersecurity and enhance privacy in their organizations. The majority of papers on this topic analyzed the security and privacy requirements of the U.S. Health Insurance Portability and Accountability Act (HIPAA) because this regulation is generally considered a significant shift in the information security management practices (Appari et al., 2009; Choi et al., 2006; M. B. Johnston & Roper, 2000). For instance, Choi et al. (2006), addressed the issues that act as barriers to the successful implementation of security measures in the context of HIPAA. However, some studies also examined health data privacy and security under the GDPR. These GDPR studies represent an essential research stream due to the high impact of GDPR on the success of digital health transformation and implementation (Mustafa et al., 2019; Pool et al., 2020).

Trust and Healthcare Compliance

Trust is a topic that is broadly studied in the healthcare literature. The majority of studies showed that cybersecurity is an essential condition of maintaining the trust of patients (Coventry & Branley, 2018). In particular, they analyzed cases in which cybersecurity relies on trust and those in which security is weakened because of a lack of trust. The existing literature advocates that privacy is also directly related to trust in the healthcare industry and that trust is a key consequence of privacy perceptions (Serenko, 2013). However, in the literature, there are no references to such considerations in healthcare compliance. The only research trend that has partially elaborated the topic is that intended for addressing trust issues towards regulations and related authorities.

An interesting observation emerging from these studies is the multi-geographical nature of the research. For example, Spronk et al. (2019) focused on the regulation of healthcare services in the Netherlands and provided insight into the elements of trust regarding regulations. Henaghan (2012) explored the trust issues in compliance environments comparatively in several countries, including the USA, Canada, Australia, New Zealand, and the UK. In a more recent study, Saechang et al. (2021) conducted cross-sectional research to examine the relationship between public trust and compliance in Thailand with particular reference to the protective measures introduced during the COVID-19 outbreak.

Contributions

While the literature is not explicit about link between trust, security, and privacy in healthcare compliance, there is an open-ended assumption of their connection. Among the precursors of this new research direction are Marotta and Madnick (2021b) who stated that "the relationship between compliance and cybersecurity can become more complicated when the privacy component is involved." In particular, they argued that some laws or regulations require organizations to implement measures with which cybersecurity is aligned, but privacy is not (or vice versa). Additionally, in another study on the subject, the authors touched upon this concept in the healthcare sector (Marotta & Madnick, 2021a). They mentioned that "there seem to be inadequate compliance procedures to communicate understandable privacy practices or provide adequate security safeguards." Thus, this paper expands on these considerations by integrating trust and privacy into the compliance versus cybersecurity "equation." In particular, this study examined the extent to which the processes established by healthcare organizations support the legal framework for the security of personal data and preserve trust and privacy in the healthcare environment.

Case Study Background: The "Barbie Incident"

In January 2018, Samantha de Jong (also known as "Barbie"), a 28-year-old Dutch reality star, was urgently admitted to the Haga Hospital (HagaZiekenhuis), one of the largest hospitals in the Netherlands (Jan Born & Floris Prenger, 2019). Following her hospitalization, a whistleblower revealed via the Publeaks website (a secure whistleblowing platform) that several hospital employees had frequently abused their position by viewing the medical file of the well-known TV celebrity. The hospital confirmed that an internal investigation had been going on since March and revealed that more than 85 employees breached a patient's privacy by illegally viewing her medical through an internal hospital system called Chipsoft. Generally, viewing private medical information is only allowed if there is medical involvement in that patient. However, the employees who accessed Samantha's file had "no treatment or care relationship with the patient," and therefore, they weren't allowed to see her medical records.

Thus, subsequently, the hospital notified the incident to the Dutch Data Protection Authority (DPA), also known as Authoriteit Persoonsgegevens (AP) (Herman Zaalberg, 2018). The notification prompted an official investigation by the AP into the hospital's data protection procedures met the requirements of the GDPR.

Aleid Wolfsen, the Dutch DPA's chairman, commented on the issue, expressing his concern about the low degree of data protection (Autoriteit Persoonsgegevens, 2019):

> *"The AP considers it a bad thing that a hospital does not have the internal security of patient records in order. A hefty fine is appropriate in this situation. The relationship between a healthcare provider and a patient should be completely confidential. Even within the walls of a hospital. It does not matter who you are."*

Thus, the incident resulted in reputational damage for Samantha as well as a severe breach of the GDPR. In particular, the investigation performed by the AP showed that the security of patient files failed in two points. Firstly, the agency found that Haga Hospital did not meet the two-factor authentication requirement or 2FA (i.e., a security feature that requires users to confirm their digital identity using two methods). Having 2FA could have validated the identification of users with legitimate access to the patient file before allowing them to access it with a code or password. Secondly, the hospital did not regularly review log files to identify unauthorized data access (Jan Born & Floris Prenger, 2019). Consequently, in July 2019, the AP imposed a fine of 460,000 euros on the Haga Hospital for insufficient security.

In order to force the hospital to enhance its security posture, the AP also imposed an order subject to a penalty on the Haga Hospital (Marianne Kolbasuk McGee, 2019). The agency stated,

"If the Haga Hospital has not improved security before Oct. 2, the hospital must pay 100,000 euros every two weeks, with a maximum of 300,000 euros."

In an attempt to address the situation, the hospital gave an official warning to the employees who viewed Samantha's files. They also responded with a statement on Twitter, Facebook, and their website (Simone Batelaan, 2019):

"Eighty-five employees of the Haga Hospital have received an official warning because they have illegally viewed the file of reality star Samantha de Jong, better known as Barbie. If they break the rules again, they will be fired immediately."

However, the Haga Hospital appealed against the fine to the AP and responded by indicating that internal security was tightened and their security measures were in place. In particular, the Haga Hospital implemented a series of measures to address the situation (e.g., mandatory e-learning courses about privacy). In addition, during the objection phase of the fine, the hospital introduced two-factor authentication and intensified logging (Maaike Kraaijeveld, 2019).

Nevertheless, the objection was declared unfounded by the regulator, and the hospital went to court. The court found it important that the hospital had taken several actions to prevent personal data from being viewed by unauthorized employees. According to the judge, these measures showed the hospital's willingness to solve their security problems in their organization. As a result, the judge said the AP did not consider this aspect, and the court reduced the fine to 350,000 euros (Hayte Hugo, 2021).

Case Study Analysis

The ramifications of the Haga breach were not limited to the consequences caused by regulatory enforcement failures. The following sections examine the main issues that emerged from the analysis of this case.

Trust and Privacy Imbalance

In examining the case, it was observed that trust and privacy were not adequately managed because there was not a "fair exchange of assets" between the patient and the hospital. Health data are considered part of a particular data category in the digital healthcare environment since they come from an individual's most personal sphere. For this reason, health data are considered the currency of health trust, which is necessary to "trade" healthcare services. Therefore, to make any medical service work, there must be sufficient mutual exposure to ensure a fair exchange of data value in both directions. On the one hand, the patient needs to provide a significant amount of personal information (trust); on the other hand, the hospital needs to maintain patient data private (privacy).

In the Haga case, the hospital did not have enough measures in place to ensure patient privacy and guarantee a fair exchange on its side. The lack of appropriate measures is also shown in the incident investigation's results, which revealed a problem hidden in the organization's roots. Mariet Bolluijt, the spokesperson for the Patient Federation, referred to this issue as a "cultural problem" concerning privacy and trust [39]. She argued that the fact that a large number of employees of the Haga Hospital viewed the medical file of reality star Samantha de Jong is a sign that the hospital lacked a culture of trust.

In particular, the absence of that culture showed that the hospital could not be trusted to handle information with privacy and trust values in mind; despite the regulations in force, employees could not resist the

temptation to view the files and failed to behave as expected. That is why there was a cultural problem, said Bolluijt (Sander van Mersbergen, 2018),

> *"Privacy is an extremely important topic. In order to make hospital staff aware of this, a lot of talking has to be done. "*

Additionally, *"the behavior of the staff is not exceptional,"* said AP spokesperson Pauline Gras (Sander van Mersbergen, 2018),

> *"Every year, we receive about ten reports from people who suspect that their personal data is being handled carelessly. We take those reports seriously: it does not matter to us whether it concerns the neighbor or a well-known Dutch person."*

Cybersecurity as a unifying factor

The investigation of the incident showed that trust and privacy were not balanced in one fundamental point: security. The hospital had poor internal security controls for patient records, which prevented the hospital from guaranteeing privacy protection and maintaining patient trust. More specifically, trust and privacy issues were mainly centered around the hospital's ability to ensure privacy through data security and the way the organization stored data.

In particular, we identified two security aspects that could have bridged the gap between trust and privacy:

1) Credentialing

Preserving privacy and trust raises challenges regarding the use and protection of data from electronic health records (EHRs) and other electronic health information (EHI) (Wang et al., 2014). One of the most essential principles of protecting private information and ensuring trust is based on access control measures. Failure to implement this principle may generate credentialing breaches (i.e., the misuse of permissions or auhorizations).

These breaches can involve unauthorized access to sensitive information, violating privacy and security restrictions. In the case of the Haga Hospital, the AP report showed that one of the security measures missing from the company's own security rules was that it was possible to log in using only a username and password (one-factor authentication) (Autoriteit Persoonsgegevens, 2019). The AP considered the one-factor authentication to be largely insufficient from a security point of view (Maaike Kraaijeveld, 2019).

In addition, the hospital failed to review log files to identify unauthorized data access regularly. In this way, the hospital failed to identify authorization issues and could not take measures against them. Implementing clear checks and monitoring would have defined the trustworthiness of the hospital and technologies within the medical context. However, legislation and regulations do not provide clear guidelines about the desired number of inspections per year (Marotta & Madnick, 2021c). The Haga Hospital failed to ensure regular audits of medical record access. Some of the causes behind this failure involved communication issues and inadequate internal organizational policies. However, the lack of regulatory clarity also contributed to aggravating this issue.

2) Internal threats

Internal actors (i.e., individuals with authorized access to an organization's sensitive data) can also cause privacy breaches – sometimes, even by the most "trusted" ones. For example, it can be an employee who mistakenly attaches a sensitive spreadsheet to an email or accidentally exposes internal passwords to external systems in plain text. Not only are internal actors the most common cause of security breach, but they are also costly to remediate, as shown from the Haga case. The medical staff that illegally viewed the celebrity's medical files acted as internal threats.

Internal threats are also partially connected to the credentialing issues described previously. For example, limiting or blocking users from accessing private information could have prevented those employees from accessing and sharing it with others.

Considering these observations, cybersecurity can be considered a unifying factor between trust and privacy. In particular, it was observed that privacy and trust relate to all principles of the Confidentiality, Integrity, Availability (CIA) Triad (Fig. 1). The CIA Triad is an information security model that shows the three main goals necessary to achieve security. In particular, it ensures that data are protected against the unauthorized use of information (confidentiality), that the accuracy and completeness of data over their entire lifecycle (integrity), and that data are available to users when they need them (availability).

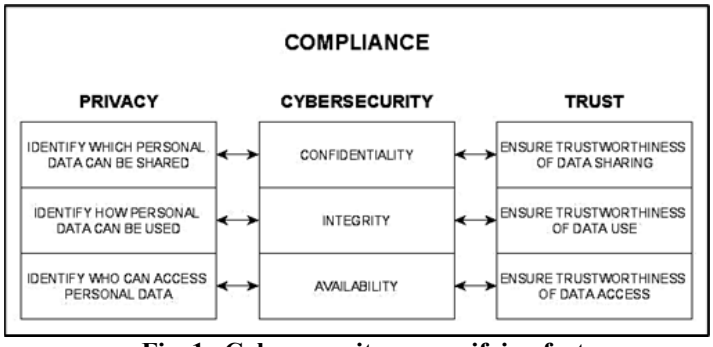

Fig. 1. Cybersecurity as a unifying factor

These three goals clearly demonstrate that the CIA Triad is entirely focused on data, which represent the most widespread assets of every company. As a result, potential threats to or failures of any of the Triad's components may have far-reaching consequences that may not be limited to cybersecurity. For example, safeguarding personal data is also a concern of privacy, which ensures the confidential use and protection of information. However, data protection can only be achieved if data (e.g., their source or content) are verified and trusted. For this reason, trust is strongly linked to the CIA Triad as it can help reduce the inherent uncertainty of cybersecurity. As a result, privacy and trust are inextricably intertwined with cybersecurity, as explained below in more detail.

Privacy relates to the CIA Triad principles in the following ways:

- **Identify which personal data can be shared**. Privacy procedures need to determine which personal information can be shared with others (confidentiality).
- **Identify how personal data can be used**. Privacy procedures need to determine how personal information is used (integrity).
- **Identify who can access personal data**. Privacy procedures need to determine who can access the data (availability).

Similarly, a trustworthy system should ensure the implementation of all three principles to a sufficient degree. In particular, the following trustworthiness principles should be satisfied:

- **Ensure trustworthiness of data sharing**. The patient trusts the hospital to share data with authorized parties (confidentiality)
- **Ensure trustworthiness of data use**. The patient trust Hospital staff do not modify data without consent (integrity)
- **Ensure trustworthiness of data access**. The patient trusts the hospital to make data available with authorized parties (availability)

Therefore, security measures that are generally undertaken to ensure the CIA Triad can be designed to preserve privacy and trust as well. For example, access control can be used as a critical requisite for ensuring trust and privacy in healthcare services.

It is also important to note that cybersecurity, and consequently privacy and trust, need to be aligned with compliance requirements, which should serve as a frame of mind for employees. However, the Haga case showed that the presence of regulations was not sufficient to ensure data protection. In addition to the issues described in the previous sections, another problem that transpired is an underlying lack of clarity in compliance requirements (The European Parliament and the Council of the European Union, 2016). This aspect means that compliance can be an unreliable substitute for preserving trust and privacy in the relationship between a hospital and its patients.

C. Comparison with the Barreiro Hospital case

The Haga incident was not the only GDPR violation in the healthcare industry. Several healthcare organizations have received fines or been subjected to regulatory actions since the regulation's enforcement in 2018. For example, on 3 December 2019, the DPA for the German state of Rhineland-Palatinate (LfDI), fined a local hospital €105.000 for inadequate organizational and technical personal data processing operations (Iannapollo, 2020). This fine was imposed in response to several GDPR violations involving patient admissions, which resulted in incorrect invoices being sent to patients and privacy issues with the hospital's management system. More recently, on October 27, 2020, the Norwegian DPA (Datatilsynet) fined the Østfold Hospital NOK750,000 (approximately €69,000) for holding health data for a prolonged period of time without applying the necessary security measures (*Norwegian DPA Imposes Administrative Fine to Østfold HF Hospital*, 2020). As a result, according to the DPA, the hospital experienced a data breach involving personal information, which mostly affected the discharge of patients from the hospital.

However, the case with the most parallels to the Haga breach is another incident that occurred at the Centro Hospitalar Barreiro Montijo (CHBM), a hospital near Lisbon, Portugal (Anna Monteiro, 2019):

In April 2018, the Sindicato dos Médicos da Zona Sul (Medical Workers Union of the Southern Zone) reported that non-clinical staff used fake medical profiles to access the hospital's computer systems. Subsequently, an investigation carried out by the Portuguese DPA (also known as the Nacional de Protecção de Dados, or CNPD), found that the CHBM did not comply with two main GDPR requirements (Luke Irwin, 2018). Firstly, the hospital violated the data minimization principle by allowing staff to unlawfully access patient data. Secondly, the CHBM failed to implement appropriate security measures to prevent unauthorized access to health data. As a result, in October 2018, the CNPD imposed a fine of €400,000 on the Barreiro Hospital (Defensorum, 2018). More specifically, the GDPR fine was broken into two parts; €300,000 for the failure to limit access to patient data and €100,000 for the failure to ensure the confidentiality, integrity, and availability of treatment systems and services.

When determining the penalty amount, the CNPD also considered the fact that the hospital took measures to address the situation. Nevertheless, the hospital contested the decision. In its defense, the hospital stated that it used the IT system provided by the Portuguese Ministry of Health to public institutions. The CNPD concluded that it was the hospital's obligation to verify that the IT system it employs is compliant with the GDPR (Anna Monteiro, 2019).

One of the most evident similarities with the Haga case involves the type of breach. Both incidents did not involve an external attack, but rather a failure to protect data access from misuse by insiders. Attorney Elizabeth Harding of the law firm Polsinelli, commented (Marianne Kolbasuk McGee, 2019),

> *"Both of these cases highlight the need to review system access to ensure that access is limited to personnel with a genuine need to know, put in place appropriate internal policies and procedures to*

enforce those access controls and offer training to ensure that personnel understand why they are in place and the implications of breaching them."

Similarly, to the situation occurred in the Netherlands, the healthcare provider-patient relationship was not built on a secure data sharing infrastructure; the security issues that emerged from the investigation were linked to excessive access to patient health records and a lack of trust in health information.

However, the two cases also presented some differences. For example, both breaches had plenty of coverage in national news outlets, but the media played a different role. In the CHBM case, the incident represented the first GDPR fine in Portugal. As a result, the story was presented by the media as an example of an example of the inaccuracies that may exist in the implementation of the security side of the GDPR. Thus, despite the repercussions of the breach, the media had a beneficial role in increasing awareness about security and compliance. Conversely, in the Haga case, the media had a more negative role, contributing to the escalation of the situation. In addition, the mediatic attention generated following the news leakage hindered the investigative procedures to some extent. For example, the hospital faced considerable pressure to complete its internal investigations as soon as possible and provide a response to the allegations made in the media. Therefore, the hospital failed to consider the situation thoroughly and overlooked possible alternative ways to manage the impact of the breach. For example, the Haga could have considered the possibility to make a preliminary notification to the competent authority. This practice is generally pursued when further investigations are needed to provide all the necessary information about a data breach or determine its occurrence. Adopting this solution would most likely have allowed the hospital to intervene more quickly in limiting or at least circumscribing the repercussions of its failures.

Results and Discussion: Lessons from GDPR Investigations

The GDPR breaches of the Haga and the CHBM provided interesting insights. The main finding is that a healthcare organization's security level can be considered an appropriate indicator for assessing the privacy and trust level in a healthcare organization. For example, by increasing the security level of information disclosure, it is possible to increase the degree of vulnerability of privacy and trust measures. In light of this finding, the three most important lessons that emerged from these cases are discussed below.

A. Security is the top priority for organizations

The two cases show that security policies and procedures should be implemented across the entire organization; otherwise, it may become difficult to control a situation promptly and adequately. For instance, the CHBM administration was aware of the vulnerabilities within their system long before CNPD conducted its investigation. Nevertheless, the hospital management decided to overlook the problem, most likely due to the amount of effort required to address it. This attitude also denoted a lack of trust in the organization's ability to ensure proper security.

B. Security is a top priority for regulators

The procedure followed by the DPAs in the two cases did not only involve issuing fines and commenting on security and privacy practices; they followed up and checked whether the hospitals had corrected their particular attention to awareness about cybersecurity and privacy by implementing mandatory training.
As a result, GDPR authorities can increase or decrease fines proportionately based on how much an organization is willing to improve its security posture (Daigle & Khan, 2020).
However, showing commitment to strengthening cybersecurity implementation may not be sufficient to demonstrate continuous security compliance. For example, many executives assume that mandatory onboarding training is automatically adequate to educate employees and sustain long-term cybersecurity behaviors. Conversely, studies found that "regular and varied training" is recommended to keep up with

evolving threats and security measures (Huang & Pearlson, 2019). Therefore, an important condition for compliance success is demonstrating the ability to make security changes effective.

C. Security is a top priority for the public

The media coverage that the incidents received showed that the general public is constantly observing the security practices adopted by healthcare organizations, especially when public interest is at stake. Therefore, security has to be a top priority for healthcare facilities to guarantee privacy and ensure that the public trusts them.

Limitations

When interpreting the results of this work and especially their applicability outside of the context of the healthcare field, it is, however, necessary to consider the limitations of the samples and data collection method. While the cases examined in this study are representative enough to investigate GDPR compliance implications, it is therefore, necessary to note that cybersecurity and compliance practices may differ from one country to another. A larger sample size could potentially lead to more accurate or comprehensive results. Additionally, this study is based on data collected from multiple public sources and scholarly works. Even though these data are sufficient to offer an accurate overview of the data breaches, incorporating primary data (e.g., interviews or surveys) might complement the research.

Implications and Conclusions

In healthcare, it is essential to ensure that cybersecurity is applied throughout the whole healthcare system, which must necessarily entail privacy protections and trust mechanisms. The analysis of the cases showed that particular attention should be placed on controls on preventing data access failures. In particular, the results revealed that, in order to have a balanced privacy-trust tradeoff, it is necessary to establish a security mechanism that ensures two main controls:

- **Limiting access to sensitive data.** This control represents an essential part of protecting data from misuse or exposure. Access controls, for example, could be designed according to the principle of least privilege, which entails granting access and permissions to a user or an application solely for a specific task. This preventive measure can help mitigate the impact of a potentially compromised user account on the company's security infrastructure.
- **Monitoring malicious activity from users with legitimate access to the organization's network.** Unauthorized access to data can be protected by using access controls, but insider threats may still pose a significant threat to data security. Thus, an organization needs to adopt measures to monitor access to and usage of data, as well as to alert security staff of activities that could jeopardize data security.

However, it is also important to note that these controls need to be managed in accordance with the applicable compliance requirements for a healthcare organization. As shown in the two cases, adhering to GDPR security requirements was not an easy task for both organizations. Whether they misinterpreted the regulation or neglected some aspects, both hospitals contested the violations by indicating that they had implemented appropriate measures. The conflicting situation originating from these disputes shows that the relationship between healthcare organizations and regulators regarding compliance appears to be adversarial in the context of security. Therefore, further investigation is needed to ensure an accurate picture of these problems and assess the considerations elaborated in this work in other healthcare contexts and geographical locations. Finally, regulatory agencies and healthcare companies may utilize this study as a tool to create more targeted cybersecurity measures and guarantee a balance between compliance, security, and privacy.

References

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Anna Monteiro. (2019). *First GDPR fine in Portugal issued against hospital for three violations*. IAPP. https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/

Appari, A., Johnson, M., & Anthony, D. (2009). HIPAA Compliance: An Institutional Theory Perspective. *AMCIS 2009 Proceedings*. https://aisel.aisnet.org/amcis2009/25

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1). https://doi.org/10.1186/S12911-020-01161-7

Autoriteit Persoonsgegevens. (2019). *Haga beboet voor onvoldoende interne beveiliging patiëntendossiers | Autoriteit Persoonsgegevens*. Autoriteitpersoonsgegevens.Nl. https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-patiëntendossiers

Ayala, L. (2016). Cybersecurity for Hospitals and Healthcare Facilities. *Cybersecurity for Hospitals and Healthcare Facilities*. https://doi.org/10.1007/978-1-4842-2155-6

Breaux, T. D., & Antón, A. I. (2008). Analyzing regulatory rules for privacy and security requirements. *IEEE Transactions on Software Engineering*, *34*(1), 5–20. https://doi.org/10.1109/TSE.2007.70746

Cellier, L., & Ghernaouti, S. (2019). An interdisciplinary approach for security, privacy and trust in the electronic medical record : A pragmatic legal perspective. *2019 IEEE International Conference on E-Health Networking, Application and Services, HealthCom 2019*. https://doi.org/10.1109/HEALTHCOM46333.2019.9009588

Choi, Y. B., Capitan, K. E., Krause, J. S., & Streeper, M. M. (2006). Challenges Associated with Privacy in Health Care Industry: Implementation of HIPAA and the Security Rules. *Journal of Medical Systems 2006 30:1*, *30*(1), 57–64. https://doi.org/10.1007/S10916-006-7405-0

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52. https://doi.org/10.1016/J.MATURITAS.2018.04.008

Daigle, B., & Khan, M. (2020). *United States International Trade Commission Journal of International Commerce and Economics The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities*. https://www.usitc.gov/journals.

Daniels, J., & Bhatia, S. (2020). Legislation and the negative impact on cybersecurity in healthcare. *ICISSP 2020 - Proceedings of the 6th International Conference on Information Systems Security and Privacy*, 691–697. https://doi.org/10.5220/0009157906910697

Defensorum. (2018). *GDPR Violation Penalty Levied Against Hospital for First Time - Defensorum*. Defensorum.Com. https://www.defensorum.com/gdpr-violation-penalty-levied-against-hospital-for-first-time/

Fan, M., Yu, L., Chen, S., Zhou, H., Luo, X., Li, S., Liu, Y., Liu, J., & Liu, T. (2020). An empirical evaluation of GDPR compliance violations in android mhealth apps. *Proceedings - International Symposium on Software Reliability Engineering, ISSRE*, *2020-October*, 253–264. https://doi.org/10.1109/ISSRE5003.2020.00032

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In *Artificial Intelligence in Healthcare* (pp. 295–336). Elsevier. https://doi.org/10.1016/b978-0-12-818438-7.00012-5

Hayte Hugo. (2021). *Rechter verlaagt AVG-boete HagaZiekenhuis tot 350.000 euro - IT Pro - Nieuws - Tweakers*. Tweakers.Net. https://tweakers.net/nieuws/180534/rechter-verlaagt-avg-boete-hagaziekenhuis-tot-350000-euro.html

Henaghan, M. (2012). Health Professionals and Trust : The Cure for Healthcare Law and Policy. *Health Professionals and Trust: The Cure for Healthcare Law and Policy*, 1–146. https://doi.org/10.4324/9780203697092

Herman Zaalberg. (2018, February). *'Tientallen snuffelden ongeoorloofd in medisch dossier Barbie' - EenVandaag*. Eenvandaag. https://eenvandaag.avrotros.nl/item/tientallen-snuffelden-ongeoorloofd-in-medisch-dossier-barbie/

Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2019-Janua*, 6398–6407. https://doi.org/10.24251/hicss.2019.76

Iannapollo, E. (2020). *Guess What? GDPR Enforcement Is On Fire!* Forrester. https://www.forrester.com/blogs/guess-what-gdpr-enforcement-is-on-fire/

Iott, B. E., Campos-Castillo, C., & Anthony, D. L. (2019). Trust and Privacy: How Patient Trust in Providers is Related to Privacy Behaviors and Attitudes. *AMIA Annual Symposium Proceedings*, *2019*, 487. /pmc/articles/PMC7153104/

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, *51*(8), 56–59. https://doi.org/10.1109/MC.2018.3191268

Iyengar, A., Kundu, A., & Pallis, G. (2018). Healthcare informatics and privacy. *IEEE Internet Computing*, *22*(2), 29–31. https://doi.org/10.1109/MIC.2018.022021660

Jackson, G. W., & Rahman, S. S. M. (2019). EXPLORING CHALLENGES AND OPPORTUNITIES IN CYBERSECURITY RISK AND THREAT COMMUNICATIONS RELATED TO THE MEDICAL INTERNET OF THINGS (MIOT). *International Journal of Network Security & Its Applications (IJNSA)*, *11*(4). https://doi.org/10.5121/ijnsa.2019.11405

Jan Born, & Floris Prenger. (2019). *Hoogste boete ooit voor HagaZiekenhuis: beveiliging na Barbie-blunder nog niet op orde - EenVandaag*. EenVandaag. https://eenvandaag.avrotros.nl/item/hoogste-boete-ooit-voor-hagaziekenhuis-beveiliging-na-barbie-blunder-nog-niet-op-orde/

Johnston, A. C., & Warkentin, M. (2008). Information privacy compliance in the healthcare industry. *Information Management & Computer Security*, *16*(1), 5–19. https://doi.org/10.1108/09685220810862715

Johnston, M. B., & Roper, L. (2000). HIPAA Becomes Reality: Compliance with New Privacy, Security, and Electronic Transmission Standards. *West Virginia Law Review*, *103*. https://heinonline.org/HOL/Page?handle=hein.journals/wvb103&id=553&div=&collection=

Luke Irwin. (2018). *Portuguese hospital appeals GDPR fine - IT Governance Blog En*. IT Governance European Blog. https://www.itgovernance.eu/blog/en/portuguese-hospital-appeals-gdpr-fine

Maaike Kraaijeveld. (2019). *Gluren in medische gegevens Barbie kost HagaZiekenhuis bijna half miljoen euro | Den Haag | AD.nl*. AD. https://www.ad.nl/den-haag/gluren-in-medische-gegevens-barbie-kost-hagaziekenhuis-bijna-half-miljoen-euro~a332a557/?referrer=https%3A%2F%2Fwww.google.com%2F

Marianne Kolbasuk McGee. (2019). *Patient Record Snooping Incident Leads to GDPR Fine – Torchsec*. Torchsec. https://www.torchsec.net/patient-record-snooping-incident-leads-to-gdpr-fine/

Marotta, A., & Madnick, S. (2021a). Convergence and Divergence of Regulatory Compliance and Cybersecurity. *Issues In Information Systems*, *November*, http://web.mit.edu/smadnick/www/wp/2020-31.pdf. https://doi.org/10.48009/1_iis_2021_10-50

Marotta, A., & Madnick, S. (2021b). Tackling Cybersecurity Regulatory Challenges: A Proposed Research Framework. In *The Role of e-Business during the Time of Grand Challenges*. Chapter 2, Volume 418 of the Lecture Notes in Business Information Processing series. Springer Nature Switzerland AG.

Marotta, A., & Madnick, S. (2021c). A Framework for Investigating GDPR Compliance Through the Lens of Security. In Jamal Bentahar, I. Awan, M. Younas, & T.-M. Grønli (Eds.), *Mobile Web and Intelligent Information Systems* (pp. 16–31). Springer, Cham. https://doi.org/10.1007/978-3-030-83164-6_2

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ (Online)*, *358*. https://doi.org/10.1136/BMJ.J3179

Mohammed, D. (2017). U.S. Healthcare Industry: Cybersecurity Regulatory and Compliance Issues. *Journal of Research in Business, Economics and Management*. www.scitecresearch.com/journals/index.php/jrbem

Mustafa, U., Pflugel, E., & Philip, N. (2019). A Novel Privacy Framework for Secure M-Health Applications: The Case of the GDPR. *Proceedings of 12th International Conference on Global Security, Safety and Sustainability, ICGS3 2019*. https://doi.org/10.1109/ICGS3.2019.8688019

Nazir, S., Ali, Y., Ullah, N., & García-Magariño, I. (2019). Internet of Things for Healthcare Using Effects of Mobile Computing: A Systematic Literature Review. *Wireless Communications and Mobile Computing*, *2019*. https://doi.org/10.1155/2019/5931315

Norwegian DPA imposes administrative fine to Østfold HF Hospital. (2020). European Data Protection Board. https://edpb.europa.eu/news/national-news/2020/norwegian-dpa-imposes-administrative-fine-ostfold-hf-hospital_en

Parker, M. (2020). Healthcare Regulations, Threats, and their Impact on Cybersecurity. *Cybersecurity for Information Professionals*, 173–202. https://doi.org/10.1201/9781003042235-9

Pool, J., Fatehi, F., Hassandoust, F., & Akhlaghpour, S. (2020). Health data privacy: Research fronts, hot topics and future directions. *Studies in Health Technology and Informatics*, *275*, 167–171. https://doi.org/10.3233/SHTI200716

Saechang, O., Yu, J., & Li, Y. (2021). Public Trust and Policy Compliance during the COVID-19 Pandemic: The Role of Professional Trust. *Healthcare*, *9*(2). https://doi.org/10.3390/HEALTHCARE9020151

Sander van Mersbergen. (2018). *"Gluren in dossier Barbie duidt op groot cultuurprobleem" | Show | AD.nl*. AD. https://www.ad.nl/show/gluren-in-dossier-barbie-duidt-op-groot-cultuurprobleem~aaf028e1/

Serenko, N. (2013). Informational, physical, and psychological privacy as determinants of patient behaviour in health care. *Handbook of Research on Patient Safety and Quality Care through Health Informatics*, 1–21. https://doi.org/10.4018/978-1-4666-4546-2.CH001

Simone Batelaan. (2019). *PRMedia&thePublic_19_20: Haga Ziekenhuis, Third Time Is the Charm?* Pytrikschafraad.Blogspot.Com. https://pytrikschafraad.blogspot.com/2019/09/haga-ziekenhuis-third-times-charm-good.html?m=0

Spronk, S., Stoopendaal, A., & Robben, P. B. M. (2019). An empirical study of how the Dutch healthcare regulator first formulates the concept of trust and then puts it into practice. *BMC Health Services Research 2019 19:1*, *19*(1), 1–10. https://doi.org/10.1186/S12913-019-4797-3

SS, B., UY, K., JM, E., K, E., S, P., D, W., S, K., M, L., S, K., D, D., & A, D. (2020). Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. *Journal of Medical Systems*, *44*(5). https://doi.org/10.1007/S10916-019-1507-Y

Strielkina, A., Illiashenko, O., Zhydenko, M., & Uzun, D. (2018). Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. *Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018*, 67–73. https://doi.org/10.1109/DESSERT.2018.8409101

The European Parliament and the Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. In *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Vaiyapuri, T., Binbusayyis, A., & Varadarajan, V. (2021). Security, Privacy and Trust in IoMT Enabled Smart Healthcare System: A Systematic Review of Current and Future Trends. *International Journal of Advanced Computer Science and Applications*, *12*(2), 731–737. https://doi.org/10.14569/IJACSA.2021.0120291

Wang, H., Sun, L., & Bertino, E. (2014). Building access control policy model for privacy preserving and testing policy conflicting problems. *Journal of Computer and System Sciences*, *80*(8), 1493–1503. https://doi.org/10.1016/J.JCSS.2014.04.017

Yuan, B., & Li, J. (2019). The policy effect of the general data protection regulation (GDPR) on the digital public health sector in the european union: An empirical investigation. *International Journal of Environmental Research and Public Health*, *16*(6), 1070. https://doi.org/10.3390/ijerph16061070