Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Comprehensive Analysis for Cybersecurity and Interoperability in Portuguese Healthcare Systems Under NIS2

Emanuel Gonçalves

Universidade Lusófona, Centro Universitário de Lisboa, Campo Grande, 376. 1749-024 Lisboa, Portugal
Email: a22404351@alunos.ulht.pt

Abstract

This article presents a comprehensive analysis of cybersecurity challenges and interoperability requirements in Portuguese healthcare systems within the context of the Network and Information Security 2 (NIS2) Directive. Drawing from data and recommendations from the European Union Agency for Cybersecurity (ENISA), the National Cybersecurity Center (CNCS), the National Data Protection Commission (CNPD), and the National Health Service (SNS), this research examines the current state of healthcare information systems in Portugal. It evaluates compliance with NIS2 requirements and proposes a framework for enhancing both security and interoperability. The research presents a set of essential practices for safeguarding patient data, emphasizing the importance of rigorous monitoring, specialized staff training, and continuous updates of security systems.

Keywords: cybersecurity; interoperability; health systems; NIS2; Portugal; European Union

Citation: E. Gonçalves, "Comprehensive Analysis for Cybersecurity and Interoperability in Portuguese Healthcare Systems Under NIS2", ARIS2-Journal, vol. 5, no. 1, pp. 38–56, May 2025.

DOI: https://doi.org/10.56394/aris2.v5i1.59

* Corresponding author. Email address: a22404351@alunos.ulht.pt

1. Introduction

The growing reliance of healthcare systems on digital frameworks renders them key targets for cyber assaults. Effective information sharing is essential for these systems to operate successfully. The 2023 Cybersecurity Report from CNCS indicates that there was a 5% increase, in cyber incidents within Portugal's healthcare sector, now reaching 8% [1],[14]. This notable rise highlights the immediate necessity for enhanced security protocols. Healthcare institutions need to focus on cybersecurity to safeguard confidential patient information and maintain uninterrupted service provision. The susceptibility of healthcare systems emphasizes the importance of strong cybersecurity measures. Interferences from cyber-attacks can jeopardize patient safety and critical medical services.

Guaranteeing interoperability is essential for delivering efficient and synchronized healthcare services. Nevertheless, ensuring safe interoperability poses considerable difficulties. Enhanced cybersecurity measures are required. The NIS2 Directive [2] establishes a crucial basis for strengthening cybersecurity regulations. Interoperability is closely linked to the NIS2 Directive. The NIS2 security guidelines facilitate safe data transmission. This illustrates how cybersecurity standards can enhance system integration. Detecting and addressing gaps represents a significant research challenge. These issues hinder the concurrent advancement of interoperability and strong cybersecurity solutions.

To successfully enhance the resilience of our healthcare systems, it is crucial to boost funding for cybersecurity infrastructure. This necessitates allocating the required resources to build robust defenses against the ever-changing cyber threats. Cooperation is essential; a strong alliance between the public and private sectors is vital for creating strategies that can anticipate and address emerging challenges. We should also focus on our frontline workers, making sure they get consistent and interactive cybersecurity training to improve their skills in identifying and addressing threats [12], [13].

Defensive strategies by themselves are not enough; they must be regularly observed and improved. Healthcare organizations should frequently evaluate their cybersecurity measures and implement required modifications. Utilizing cutting-edge technologies such as artificial intelligence and machine learning can greatly improve our capacity to quickly recognize and tackle threats. Ultimately, it is essential to have clear and practiced strategies for addressing cyber incidents. This readiness guarantees that, when an attack happens, we can reduce interruptions to patient care and swiftly resume delivering the highest quality of service.

1.1. Research Objectives

This study looks at the present cybersecurity and interoperability status in Portuguese healthcare systems. It assesses compliance with NIS2 and suggests improvements. The recommendations are based on findings from ENISA and CNCS. Key Research Objectives are to:

- Cybersecurity Evaluation: Assess current cybersecurity measures and identify vulnerabilities in healthcare systems.

- Interoperability Analysis: Examine current interoperability standards and practices within the SNS framework.
- NIS2 Compliance Assessment: Evaluate the impact of NIS2 compliance on data security and system integrity.
- Solution Proposals: Develop strategies to improve cybersecurity and interoperability based on ENISA and CNCS guidelines.
- Recommendations: Suggest best practices for implementing security and interoperability improvements effectively.

2. Background

2.1. Portuguese Healthcare System Structure (SNS)

The SNS Digital Strategy for 2023-2026 [3] aims to transform healthcare in Portugal through digitalization. It focuses on deploying electronic health records (EHR) and tools to improve communication. The strategy plans to merge hospital units and health clinics for better accessibility. This program promises a modern and connected healthcare environment for patients and staff [14].

- SNS Digital Strategy to 2023-2026:

At the conference held in Lisbon on April 18, 2023, the Minister of Health emphasized that digitalization aims to serve people and healthcare professionals, improving access and system sustainability. He mentioned several digital tools already implemented, such as automatic prescription and teleconsultations, highlighting the importance of the Recovery and Resilience Plan (PRR), with an investment of 300 million euros for digitalization.

The SNS Digital Strategy 2023-2026 aims to modernize healthcare in Portugal. A major focus is on the digitalization of patient records. This involves the implementation of an Electronic Health Record (EHR) system. The unified EHR will streamline patient data management. It will improve communication between healthcare providers. Consequently, the quality of healthcare delivery will be enhanced. This strategy also includes significant investments in technology. Additionally, it aims to integrate hospital units and health centers. The ultimate goal is a more efficient and accessible healthcare system.

This strategy involves the integration of 39 hospital units and 55 Health Centers Group (ACES). This initiative aims to enhance coordination across various healthcare entities [14]. A unified system will streamline patient information sharing. Healthcare providers can access complete medical records more efficiently. This will reduce redundancies in patient care. Improved communication will ensure timely medical interventions. Integrated

systems promote better resource management. Overall, it will lead to a more cohesive healthcare system. Patients will benefit from continuity of care.

- Current Digital Infrastructure

The current digital infrastructure includes the RSE (Registo de Saúde Eletrónico) platform. This platform centralizes patient health records and ensures accessibility for healthcare providers. The RSE improves efficiency in managing health data. Health professionals can easily access comprehensive medical histories [15]. This leads to better-informed clinical decisions. The platform enhances coordination among various health services. It also supports the integration of new digital tools. Overall, the RSE contributes to a modernized healthcare system.

Portugal's healthcare system includes the PEM (Prescrição Eletrónica Médica) system. This digital tool manages electronic prescriptions for medications, centralizing and simplifying the entire prescription process. Health professionals can quickly generate and manage these prescriptions. Patients receive their prescriptions digitally and can access them easily. This process reduces errors and enhances overall efficiency in healthcare, ensuring secure transmission of prescription data. It supports integration with other digital healthcare tools and improves the quality of services provided to patients [16].

The SDM (Sistema de dados Mestre) is a vital tool in healthcare data management, integrating reference information to organize the healthcare system and other information systems. It ensures data standardization and enhances data quality, facilitating quick access to centralized information for various entities. Currently, around 6,000 users of the SNS benefit from its capabilities.

The Local Integration Gateway for Healthcare (LIGHt) is the Local Integration Platform of the Shared Services of the Ministry of Health (SPMS). It functions as an integration layer that facilitates the secure exchange of information between internal and external systems. By using open-source technologies, LIGHt promotes data normalization and security, enabling audits and preventing unauthorized access. Its goal is to provide a reliable and highly configurable integration mechanism, enhancing local and national interoperability. The platform supports communication via Health Level 7 (HL7) and HL7 Fast Healthcare Interoperability Resources (FHIR), ensuring the unification of local systems and facilitating future integrations. With LIGHt, SPMS aims to align workflows and prevent errors, focusing on patient care. Eliminating direct access to databases increases system security and reliability [11], [17]. The Portuguese National Broker (PNB), part of this system, centralizes the transfer of health data, promotes interoperability, and improves workflow maintenance. It integrates various projects and products, ensuring secure access control in message exchanges between systems. Currently, PNB processes an average of 500,000 daily messages, facilitating communication across multiple interfaces and enhancing healthcare coordination.

"Exames Sem Papel" is an initiative by the Ministry of Health to digitize the processes related to Complementary Means of Diagnosis and Therapeutics (MCDT), ensuring that all information follows the patient digitally. This project aims to strengthen the interaction between doctors and patients, reduce waste in MCDT services, decrease bureaucracy, and enhance security for all involved. By providing digital results to both doctors

and patients, it incorporates measures to protect against unauthorized or illegal data processing during digital result sharing. Simplifying the MCDT requisition process is essential, moving from an article-based model to a digital one while allowing patients the option to retain article records. This approach ensures the project's success and efficiency gains for the National Health Service (SNS), offering greater convenience for both citizens and healthcare professionals.

The National Epidemiological Surveillance System (SINAVE) digitizes the notification of mandatory reportable diseases. It interacts with infection surveillance systems, offers electronic forms for notification registration, and sends alerts to authorities. SINAVE integrates with the European Surveillance System (TESSY), providing data and statistics to the Directorate-General of Health (DGS). Benefits include improved data quality, patient privacy protection, increased notifications, and reduced information processing time [7], [8].

2.2. NIS2 Directive Framework

The NIS2 directive [2], an advancement of NIS1, introduces a new approach to EU cybersecurity. NIS1 established the basic cybersecurity requirements and facilitated interaction between member countries. However, as cyber-attacks evolved, NIS2 became the new standard. With various sectors like healthcare, energy, and transportation enhancing their infrastructure, NIS2 addresses the expanded cyber threat landscape. Its flexible approach covers more sectors, offering a more efficient application of EU-wide cybersecurity policies and upgrading security requirements [9], [10].

A key feature of NIS2 is its focus on enhancing risk management and reporting duties. Businesses must adopt advanced protection and continuously assess their cyber risk exposure. Incident reporting is now mandatory within 24 hours, enabling quicker and more detailed responses. Implementing the directive is crucial for secure interoperability in Portuguese healthcare systems. The guidelines promote an integrated approach to tackle cybersecurity challenges, with risk management measures and supply chain security assessments.

Continuous training in cybersecurity practices and creating clear policies for managing risks and incidents are necessary. Fostering a cybersecurity culture among all stakeholders and collaboration among healthcare institutions, technology providers, and governmental entities is vital. This ensures healthcare systems protect against cyber threats and operate efficiently. In summary, NIS2 is not just a legal obligation but an opportunity to enhance security. Proper implementation improves resilience, increases patient trust, and enhances service effectiveness.

2.3. Data Protection Requirements

The General Data Protection Regulation (GDPR) [4] significantly improved data protection and privacy in the European Union. Within this framework, the regulation requires rigorous monitoring of patient data to high

standards. It gives individuals the right to access, correct, and delete their data, ensuring protection. Furthermore, enterprises must demonstrate compliance with GDPR principles by implementing strong data security measures.

GDPR also adds the notions of "privacy by default" and "privacy by design." Healthcare software frequently fails to meet regulatory requirements, affecting total compliance. The regulation increases the right to data portability, which would become less important with improved system integration. Given the sensitivity of the data processed by the National Health Service (SNS), compliance is critical. Hospitals and private services, including labs and imaging centers, must follow GDPR guidelines strictly for data security.

Data protection has become paramount in information management, particularly in the healthcare sector. Safeguarding patient data is a legal and ethical commitment. This chapter highlights some of the critical points for data protection, with an emphasis on methods for protecting patient data, cross-border data transfer protocols, and consent management systems.

- Encryption Requirements for Sensitive Data

Encryption is also a crucial aspect of data security, ensuring that, in the event of unauthorized access or interception, the data remains unreadable and protected. This principle applies to data in transit, utilizing secure communication protocols, and at rest, where data must be encrypted with strong algorithms. Only those possessing the decryption key can effectively access the actual content.

- Access Controls

To ensure that only authorized personnel have access to patient data, it is necessary to have access control systems in place. This control should be implemented based on profiles assigned according to user permissions. Multi-factor authentication should also reinforce these access controls, minimizing the likelihood of unauthorized access and subsequent data breaches.

- Audit Trails Implementation

Audit trails comprising access information, are fundamental for monitoring and tracking all accesses and potential modifications to patient data. These records provide detailed data on who accessed the information when access occurred, and what actions were taken by the user. They also enable the detection of suspicious activities and facilitate legal or forensic investigations in case of data breaches.

- Cross-Border Data Transfer Protocol

Cross-border patient data transfers are required by the globalization of healthcare services, which presents serious privacy and security issues. The GDPR, which establishes guidelines for the transfer of personal data outside the EU, must be followed by European organizations, including those in the healthcare industry. Protecting

patient data during cross-border transfers requires that protocols and contracts contain data protection impact assessments and contractual terms.

- Consent Management

Consent for processing personal data is one of the pillars of the GDPR, requiring explicit individual permission. This consent must be free, specific, informed, and unequivocal, with clear and accessible requests. Individuals have the right to withdraw consent at any time, and organizations must facilitate this process. The use of consent management systems is important and must have a user-friendly interface. This ensures that users with low literacy and computer experience can withdraw or renew consent. Ensuring proper consent promotes transparency, trust, and respect for data subjects' rights, ensuring GDPR compliance

3. Current State Analysis

3.1. Cybersecurity Assessment

The current state analysis of cybersecurity in healthcare shows significant vulnerabilities. According to the CNCS report, prepared and made available in July 2024 [1], regarding the risks and conflicts of 2023, with statistical data from the national landscape, it reveals a concerning panorama about cybersecurity in the health sector. For a better understanding of the issue, some of these data are presented below:

- Security Incidents

In 2023, the health sector was the target of 171 security incidents, standing out as one of the most vulnerable to cyber-attacks, ranking 3 places in the top 10 [1:29]. The complexity and the amount of sensitive data present in this sector make it an attractive target for cybercriminals. These incidents range from minor system disruptions to significant failures that compromise data integrity.

- Ransomware Attacks

Out of the reported cases, 2 were linked to ransomware attacks, in the health sector [1:8], which remain among the most common threats. These attacks prevent data access until a ransom is submitted, leading to major interruptions in health services. Interestingly, this goal is nonsensical since public institutions will never pay ransoms. Bouncing back from a ransomware attack can be both lengthy and expensive, impacting the hospital's capacity to deliver sufficient care to patients.

- Data Breaches

Data breaches represent 4 places and account for 11% of reported incidents [1:46], involving unauthorized access to sensitive information. These breaches can result in the theft of personal and medical data, exposing patients to identity theft risks. More severe cases can even alter records in diagnosis and treatment. Insufficient

data protection makes these breaches particularly concerning, requiring robust security measures to prevent unauthorized access.

- Phishing Attempts

Phishing attempts account for 3 incidents [1:33], where cybercriminals try to deceive employees to obtain confidential information. These attempts often use fraudulent emails or messages that mimic legitimate communications. Continuous training of staff in secure cybersecurity practices is essential to recognize and avoid these attacks.

- Other Security Incidents

Finally, the other security incidents encompass a range of additional threats, including malware and DDoS assaults. While occurring less often, these incidents can still lead to major service disruptions and jeopardize data security. Establishing a thorough security plan is essential to alleviate the dangers linked to these various threats.

3.2. SNS Digital Infrastructure

The SNS Digital Infrastructure has made significant progress in modernizing Portugal's healthcare systems. All public hospitals with integrated EHR systems are considered part of the service, according to the OECD report [5], Portugal is one of the countries that has a country-wide eHR system. The Shared Services of the Ministry of Health (SPMS), responsible for infrastructure and systems, provide this possibility to all SNS institutions. Examples include PEM systems, paperless prescriptions, and paperless exams.

This service also developed telemedicine functionality, enabling teleconsultations between doctors and patients, allowing for remote consultations and improved patient access to medical care. Access has been available through the SNS.24 portal or app since December 17, 2024. Consequently, there is no statistical data yet to evaluate the service's performance. However, some limitations can be noted. To function effectively, particularly on the doctors' side, certain technical conditions are necessary, such as computers, internet, microphones, and cameras. Not all offices meet these requirements.

Regarding the use of the FHIR standard in new systems, although no specific information is available, it can be stated that a significant portion of the systems still rely on the HL7 standard, mostly version 2.5. This aspect requires considerable improvement. These advancements demonstrate a commitment to enhancing healthcare through digital transformation initiatives. The integration of these technologies streamlines processes and improves overall patient care. Ongoing efforts aim to achieve even greater digital integration shortly.

3.3. ENISA Risk Assessment Framework

ENISA has developed a Risk Assessment Framework to improve the cybersecurity resilience of organizations. Within this framework, several critical vulnerabilities have been identified that must be addressed to ensure robust

security measures. These vulnerabilities include the integration of legacy systems, insufficient security training, outdated security protocols, and non-compliant data storage practices.

- Integration of Legacy Systems [6:17]

Legacy systems pose significant challenges due to their outdated technologies and lack of support for modern security standards. Integrating these systems with contemporary IT infrastructure often leads to security gaps, increasing the risk of cyberattacks. Organizations, particularly hospitals, must prioritize the modernization or secure isolation of legacy systems to effectively mitigate these risks.

- Insufficient Security Training [6:22]

Another pressing vulnerability is the lack of comprehensive security training for employees. Human error remains a primary factor in many cybersecurity breaches, often resulting from inadequate awareness and understanding of security best practices. Implementing regular security training programs is essential to equip employees with the knowledge and skills necessary to identify and respond to potential threats.

- Outdated Security Protocols [6:27]

Outdated security protocols can leave organizations vulnerable to cyberattacks. As cyber threats evolve, security measures must also evolve to defend against them. Relying on obsolete protocols can render even the most sophisticated systems susceptible to breaches. It is imperative that hospitals continually update and refine their security protocols to align with the latest industry threat standards.

- Non-Compliant Data Storage

Data storage must adhere to regulatory standards. Failure to do so can lead to severe legal and financial repercussions, as well as exposing sensitive information to unauthorized access. Hospitals and related organizations must ensure that all data storage solutions meet compliance requirements and incorporate strong encryption and access controls.

In conclusion, addressing these key vulnerabilities integration of legacy systems, insufficient security training, outdated security protocols, and non-compliant data storage is crucial for organizations to improve their cybersecurity posture. Adhering to the ENISA Risk Assessment Framework will enable them to effectively identify and mitigate risks, thereby protecting their information assets and maintaining regulatory compliance.

4. Compliance Analysis

4.1. NIS2 Readiness Assessment

Portugal has not yet transposed the NIS2 directive, missing the established date of October 17, 2024. However, a public consultation began on November 22, 2024, and was extended until December 31, 2024, aiming to gather

opinions on the new legal regime. By the end of 2025, the Portuguese government aims to complete this transposition to avoid further fines.

In Europe, some countries comply, and others have already started the process. Below is a table showing the countries and their state of completion (Preliminary, In progress, or Completed)

Table 1: Implementation Status of NIS2 in the European Union

Country	Preliminary	In progress	Completed
Austria		■	
Belgium			■
Bulgaria	■		
Croatia			■
Cyprus		■	
Czech Republic		■	
Denmark		■	
Estonia	■		
Finland		■	
France		■	
Germany		■	
Greece		■	
Hungary			■
Ireland		■	
Italy		■	
Latvia			■
Lithuania		■	
Luxembourg		■	
Malta	■		
Netherlands		■	
Poland		■	
Portugal	■		
Romania		■	
Slovakia			■
Slovenia		■	
Spain	■		
Sweden		■	

Preliminary: Sparse information available or limited advancement

In Progress: "Early stages of development with some advancements achieved, or the draft has been submitted and is awaiting feedback or approval.

Completed: Transposition of NIS2 into national law

4.2. GDPR Compliance Status

Portugal has guaranteed adherence to the GDPR, especially in organizations associated with the SNS. Every one of these institutions employs its own Data Protection Officer (DPO), who has been undertaking a notably difficult role.

Healthcare organizations encounter a complicated environment, featuring various processes, numerous information systems, extensive data, and a significant number of users. This intricacy requires ongoing time, effort, and commitment from DPOs to maintain adherence to GDPR standards. Nonetheless, since most DPOs are direct staff members of the organizations, they might not always have the required independence to carry out their roles completely on their own. Despite this challenge, it is thought that the essential compliance standards are fulfilled, guaranteeing sufficient protection of personal data for both patients and staff. Unfortunately, there is no useful information available on the CNPD portal to validate these conclusions.

5. Recommendations

5.1. Security Enhancement (ENISA Framework)

Technical Measures

To enhance security protocols, it is vital to utilize multi-factor authentication and encryption methods. Incorporating sophisticated threat detection systems can actively recognize and eliminate possible threats. Furthermore, routine security assessments guarantee adherence and reveal opportunities for enhancement.

- Network segmentation [6:24]

Network segmentation is a tactic employed to restrict the propagation of threats throughout the IT framework. Dividing the network into smaller, separate sections can help lessen the effects of a possible attack. This action greatly enhances the system's overall resilience.

- Advanced Endpoint Protection

Sophisticated endpoint protection entails deploying security measures that exceed the capabilities of conventional antivirus programs. Technologies like endpoint detection and response (EDR) facilitate the detection

of questionable activities and prompt action in response to incidents. These instruments are essential for safeguarding devices from sophisticated dangers.

- 24/7 Security Monitoring [6:36]

Continuous security surveillance enables the proactive identification of threats and the swift reaction to incidents. Security operations centers (SOC) function around the clock to guarantee that any unusual activity is rapidly detected and resolved. This method is essential for preserving system integrity. Ideally, every hospital unit ought to dispatch an automated activity report to a centralized security operations framework within SPMS.

- Automated Incident response [6:31-33]

Automated incident response employs technologies like security orchestration, automation, and response (SOAR). This method enables the swift and accurate implementation of mitigation measures without human involvement. Automating incident response shortens response time and lessens the effects of attacks.

Organizational Measures

Establishing strong organizational practices is essential for maintaining security and efficiency. Creating clear policies and procedures, alongside frequent staff training, aids in upholding compliance and preparedness. Additionally, promoting a culture of ongoing improvement and responsibility strengthens overall organizational resilience.

- Security Awareness Training [6:22]

Ongoing security awareness training is essential to guarantee that every employee understands threats and cybersecurity best practices. Consistent training sessions contribute to the development of a security culture in the organization. All employees must understand their part in safeguarding information assets since cybersecurity relies on each individual.

- Incident Response Procedures [6:31-33]

Creating clear and specific incident response protocols is essential for efficiently handling cybersecurity emergencies. These procedures ought to encompass communication strategies, allocation of roles, and specific

actions for containment and recovery. Consistently engaging in these procedures via simulations can greatly enhance the organization's preparedness.

- Business Continuity Planning [6:34]

Business continuity planning guarantees that the organization can keep functioning despite disruptive events. This plan must pinpoint essential processes and establish recovery tactics to reduce downtime. Maintaining business continuity is crucial for the resilience of organizations.

- Supply Chain Risk Management [6:53]

Security in the supply chain is an essential aspect that is frequently overlooked. It is essential to ensure that suppliers and partners adhere to security standards to safeguard the integrity of data and systems. Enforcing supply chain risk management strategies can avert breaches that impact the organization. In the domain of D1: Governance and Risk Management, see ISO 27036-3, Part 3, which provides guidelines for ICT supply chain security.

5.2 Interoperability Framework

Technical Standards

To ensure seamless and secure communication between diverse healthcare systems, the SNS guidelines outline a comprehensive interoperability framework. This framework focuses on implementing technical standards that facilitate efficient data exchange and improve patient care coordination. Below are the key components:

- FHIR Implementation: Adopt the FHIR standard to enhance the exchange and interoperability of healthcare information. This adoption can facilitate more efficient data sharing between systems, benefiting patient care coordination. FHIR, utilizing RESTful APIs and JSON, standardizes health data sharing, boosting innovation and collaboration. As an open web-based standard, it enables seamless communication between healthcare systems, improving care quality and reducing costs. Its flexibility allows custom profiles, making it adaptable for diverse healthcare settings.

- HL7 v2.5 Migration: The migration of existing systems to HL7 version 2.5 is essential to ensure compatibility with the latest healthcare information exchange standards. This action will result in greater data accuracy and consistency, thereby improving integration with modern healthcare IT solutions.

- API Security Requirements: Comprehensive security requirements for APIs should be established to protect sensitive healthcare data. This should occur during the data exchange and integration

processes, involving robust authentication, authorization, and encryption mechanisms. This will safeguard data integrity and confidentiality.

- Data Exchange Protocols: Developing and implementing standardized data exchange protocols is key to ensuring continuous and secure communication between healthcare systems. These protocols should enable efficient data interoperability.

Operational Procedures

To enhance the organization's security, data management, and overall efficiency, it is crucial to implement specific operational procedures. These procedures ensure that healthcare platforms are secure, reliable, and efficient.

- Cross-System Authentication: Implement cross-system authentication to ensure secure access across various healthcare platforms. This measure will streamline user management while enhancing overall security. It also helps in reducing redundant user accounts and associated administrative overhead.

- Data Quality Assurance: Establish rigorous procedures to maintain the accuracy and reliability of healthcare data. Regular quality checks are essential to uphold the integrity and usefulness of the exchanged information. Additionally, employing automated tools for data validation can significantly reduce errors and improve efficiency.

- Service Level Agreements: Develop and enforce service level agreements (SLAs) that define expected performance and availability of healthcare IT services. SLAs help ensure accountability and consistent service delivery.

- Change Management Processes: Introduce robust change management processes to handle system updates and modifications efficiently. This approach minimizes disruptions and maintains system integrity during changes.

5.2. Implementation Roadmap

Based on CNCS recommendations, Phase 1 (Q2-Q3 2024) focuses on the following actions:

- Risk Assessment Finalization: To find possible security flaws and dangers, carry out a comprehensive risk assessment. This will entail assessing current assets, procedures, and systems to identify risk areas and ranking them according to their possible consequences.

- Creation of a Security Baseline: Create and implement a security baseline that specifies the minimal security procedures and standards that the company must adhere to. Over time, the security posture will be measured and improved using this baseline as a guide.

- Launch of Staff Training: Start educating employees on cybersecurity best practices as well as the particular security rules and procedures of the company. All staff members will be guaranteed to understand their duties and responsibilities in upholding a secure workplace thanks to this training.

- First Compliance Assessment: To make sure that pertinent laws, rules, and standards are being followed, perform an initial compliance assessment. To guarantee complete regulatory compliance, identify any shortcomings or non-compliance areas that require correction.

This phase establishes the groundwork for a strong cybersecurity framework by concentrating on crucial elements including risk management, security standards, staff training, and regulatory compliance. The company

may improve its overall security posture and successfully safeguard its resources and data by systematically putting these measures into place.

Regarding Phase 2 (Q4 2024-Q1 2025), we have another set of actions, such as:

- Safety Procedures Implementation: To fix vulnerabilities found and improve the organization's security posture, carry out the planned security actions. Make sure these steps are easily incorporated into the current procedures and systems.

- Improvements in Interoperability: Boost system and application compatibility to guarantee smooth data interchange and communication. This will enable safer and more effective operations throughout the company.

- Process Documentation: Provide thorough documentation of all security processes and procedures. Staff members will be able to refer to this material, which will also help with continuous training and attempts to increase compliance.

- Compliance Monitoring Setup: To continuously assess compliance with pertinent laws and standards, set up a compliance monitoring system. This method will assist in quickly identifying and resolving compliance issues.

The company may strengthen its security architecture, increase operational effectiveness, and guarantee continued regulatory compliance by methodically putting these procedures into practice.

And in the final, Phase 3 (Q2-Q4 2025), to conclude, we have the following actions:

- Achieving Complete NIS2 Compliance: Ensure that your entity is fully compliant with the NIS2 Directive, meeting all required parameters. This action will not only enhance regulatory compliance but also strengthen the organization against cyber threats.

- Implementation of Advanced Security Features: Adopt enhanced security measures to bolster the organization's protective capabilities. These measures should be integrated into the existing security framework for maximum effectiveness.

- Continuous Improvement Program: Propose the implementation of a continuous improvement initiative aimed at optimizing security processes and methodologies. Firewall protocols must be updated and revised at regular intervals to address emerging threats.

- Audit Procedures: Establish regular audit procedures to systematically evaluate and review security measures. These audits should ensure ongoing compliance and help identify areas requiring intervention.

By meticulously following these steps, the organization can build a robust security structure and maintain high compliance standards. Moreover, it will have the opportunity to continuously improve its IT security strategy.

6. Conclusion

The establishment of the NIS2 directive is imperative for obtaining secure interoperability in Portuguese healthcare systems. The directive outlines an integrated methodology, which is essential to face common cybersecurity issues in this domain. In terms of the analysis, significant advancement has been noted in the transformed face of digital health within Portugal. Nevertheless, there are quite critical areas that need an urgent address for the compliance of NIS2.

The implementation of effective NIS2 will be a critical factor for security in healthcare systems and the protection of patients' data. This structured approach adds to the CNCS through the security framework of ENISA and SNS interoperability guidelines. Furthermore, health professionals should receive continuous training in cybersecurity, and clear policies should be developed concerning the management of risks and incidents. An integrated approach means that all stakeholders foster not just technical measures but a cybersecurity culture.

This calls for collaboration among healthcare institutions, technology providers, and governments to ensure that healthcare systems are not only secure but also operate smoothly and efficiently. Continuous training, knowledge sharing, and regular audits will lead to ongoing compliance with NIS2. In short, NIS2 is more than a legal obligation but an opportunity to step up when it comes to security. Proper implementation can enhance resilience in healthcare systems. This might also be a competitive advantage and therefore enhance patients' trust in the services.

References

[1] ENISA. (2024, Jul) "Relatório Cibersegurança em Portugal - Riscos e Conflitos – 5.ª edição". [On-line]. Available: https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs.pdf [Dec. 14, 2024].

[2] Official Journal of the European Union. (2022, Dec 14) "Directive (Eu) 2022/2555 of the European Parliament and of the Council". [On-line]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555 [Dec. 16, 2024].

[3] Serviço Nacional de Saúde. (2023, Apr 19) "Transição Digital na Saúde". [On-line]. Available: https://www.sns.gov.pt/noticias/2023/04/19/transicao-digital-na-saude-2/ [Dec. 17, 2024].

[4] Official Journal of the European Union. (2016, Apr 27) "Regulation (Eu) 2016/679 of the European Parliament and of the Council". [On-line]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Dec. 16, 2024].

[5] OECD. (2021, Sep 17) "Progress on Implementing and Using Electronic Health Record Systems: Developments in OECD Countries as of 2021". [On-line]. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/progress-on-implementing-and-using-electronic-health-record-systems_f6c2a59a/4f4ce846-en.pdf [Dec. 18, 2024]

[6] ENISA. (2021, Jul.) "Guideline on Security Measures Under the EECC – 4th Edition". [On-line]. Available: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20-%20Guideline%20on%20Security%20Measures%20under%20the%20EECC-%204th%20edition.pdf [Dec. 28, 2024]

[7] Mateus-Coelho, Nuno, and Manuela Cruz-Cunha, editors. Exploring Cyber Criminals and Data Privacy Measures. IGI Global, 2023. https://doi.org/10.4018/978-1-6684-8422-7

[8] Mateus-Coelho, Nuno Ricardo, et al. "POSMASWEB: Paranoid Operating System Methodology for Anonymous and Secure Web Browsing." Handbook of Research on Cyber Crime and Information Privacy, edited by Maria Manuela Cruz-Cunha and Nuno Mateus-Coelho, IGI Global, 2021, pp. 466-497. https://doi.org/10.4018/978-1-7998-5728-0.ch023

[9] Mateus-Coelho, N. (2021). A New Methodology for the Development of Secure and Paranoid Operating Systems. Procedia Computer Science, 181, 1207-1215. https://doi.org/10.1016/j.procs.2021.01.318

[10] R. Neware and A. Khan, "Cloud Computing Digital Forensic challenges," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018, pp. 1090-1092, [Online]. Available: 10.1109/ICECA.2018.8474838.

[11] Z. AlSaed, M. Jazzar, A. Eleyan, T. Bejaoui and S. Popoola, "An Integrated Framework Implementation For Cloud Forensics Investigation Using Logging Tool," 2022 International Conference on Smart Applications, Communications and Networking (SmartNets), Palapye, Botswana, 2022, pp. 01-06, [Online]. Available: 10.1109/SmartNets55823.2022.9994001.

[12] G. Chen, D. Wu, G. Chen, P. Qin, L. Zhang and Q. Liu, "Research on Digital Forensics Framework for Malicious Behavior in Cloud," 2019 IEEE 4th Advanced Information Technology, Electronic and Automation

Control Conference (IAEAC), Chengdu, China, 2019, pp. 1375-1379, [Online]. Available: 10.1109/IAEAC47372.2019.8997702.

[13] S. N. Joshi and G. R. Chillarge, "Secure Log Scheme for Cloud Forensics," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 188-193, [Online]. Available: 10.1109/I-SMAC49090.2020.9243428.

[14] M. Dave, "Internet of Things Security and Forensics: Concern and Challenges for Inspecting Cyber Attacks," 2022 Second International Conference on Next Generation Intelligent Systems (ICNGIS), Kottayam, India, 2022, pp. 1-6, [Online]. Available: 10.1109/ICNGIS54955.2022.10079829.

[15] J. Song and J. Li, "A Framework for Digital Forensic Investigation of Big Data," 2020 3rd International Conference on Artificial Intelligence and Big Data (ICAIBD), Chengdu, China, 2020, pp. 96-100, [Online]. Available: 10.1109/ICAIBD49809.2020.9137498.

[16] S. Jilani, N. N. Kishore, N. N. Chand, R. D. Varma, G. Raja and P. V. Rao, "Big Data Security: Detect and Prevent the Data from Attacks with Digital Forensic Tools," 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2023, pp. 783-787, [Online]. Available: 10.1109/ICSSIT55814.2023.10060947.

[17] S. Ozcan, M. Astekin, N. K. Shashidhar and B. Zhou, "Centrality and Scalability Analysis on Distributed Graph of Large-Scale E-mail Dataset for Digital Forensics," 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 2020, pp. 2318-2327, [Online]. Available: 10.1109/BigData50022.2020.9378152.