RESEARCH PAPER

The adoption of a cybersecurity framework in a healthcare, surgical and oncological environment: “synergy-net” a campania fesr-por (European fund of regional development - regional operative program) research project

Domenico Parmeggiani[1*], Mattia Siciliano[2], Giancarlo Moccia[1], Pasquale Luongo[1], Francesco Miele[1], Francesco Torelli[1], Pasquale Sperlongano[1], Stefano Marrone[3], Michela Gravina[3], Carlo Sansone[3-4], Ruggiero Bollino[5], Paola Bassi[1], Antonella Sciarra[1], Maddalena Claudia Donnarumma[1], Chiara Colonnese[1], Simona Parisi[6], Chiara Lanza Volpe[6], Nadia De Falco[1], Ludovico Docimo[6] and Massimo Agresti[1]

Abstract

As with any other sector, the healthcare industry is also prone to cyber threats. Though the nature of threats is similar to any other industries, it does need to address sector-specifics risks along with security risks in its operating environments. Every day the Hospitals need to ensure that the information is adequately secured. Currently Chief Information Officer (CIOs) and Chief Information Security Officer (CISOs) are trying to protect their hospital Information Systems (IS) departments from security threats. Itis imperative to take necessary measures to ensure risk management and business continuity. The Paper addresses some of the challenges faced by healthcare organizations in the selection of a Cyber Security Framework by reviewing some of the common standards and frameworks that are used by healthcare organizations. The also paper highlights the advantages and disadvantages of each of the standards as: International Organization for Standardization (ISO)/IEC 27799, Health Insurance Portability and Accountability Act (HIPAA), HITRUST, Nation Institute of Standards and Technology (NIST) has developed the Cyber Security Framework (CSF) and General Data Protection Regulation (GDPR) and compare and the additional directives provided by this standards.

Keywords: information security management systems, health information security, HIPAA, NIST CSF, CISO

Introduction

The fourth industrial revolution heralds a new chapter in the story of how modern healthcare is evolving. The global challenges of new chronic disease epidemics, clinical labor shortage and spiraling costs will need to be met head-on by new digital means of providing personalized care to the masses. Macro-trend innovations will radically transform healthcare provider business and operating models through a powerful and profound set of innovative technologies.

Precision and genomic medicine, real-time clinical operation, virtual care, population health and care pathway orchestration platforms are emerging and converging to form hyper-connected digital services and smart infrastructure that form the new healthcare delivery model.

The benefits of this transformation will be a more integrated network of care within and across health providers and professional teams [1]. With Healthcare organizations increasingly finding the need to reassure their customers and regulators that their devices have incorporated adequate security measures, there is a growing demand to comply their organization’s security with various recognized security frameworks and standards. Though numerous standards and set structures available in the market, selection of the right framework to meet the organization’s need has become a challenge as organization shave to deal with various concerns related to these frameworks like standard inconsistencies, lack of prescriptiveness, compliance, cost, complexity, and certifications [2]. Chief Information Officer (CIOs) / Chief Information Security Officer (CISOs) should perceive these innovation trends

[1]Integrated Activity Department of Surgery, Orthopedics and Hepatogastroenterology, University of Study of Campania “Luigi Vanvitelli” Naples, Italy

[2]Chief Operation Officer of Practice of Forensic-Investigation, Defense and Telecommunications, President of the Cyber Security Committee of the Order of Engineers Naples, Italy

[3]DIETI, University of Naples Federico II, Naples, Italy

[4]CINI, ITEM Laboratory “C.Savy”, Via Cintia 21, Naples, Italy

[5]Bollino IT S.p.A., Via delle Industrie 31, Naples, Italy

[6]Highly Specialized Medical-Surgical Department of the University of Campania "Luigi Vanvitelli" Hospital Naples, Italy

**Author for correspondence: domenico.parmeggiani@unicampania.it*

Received: 26 August, 2023, Manuscript No. fmcp-23-111300, **Editor assigned:** 29 August, 2023, PreQC No. fmcp-23-111300 (PQ), **Reviewed:** 06 September, 2023, QC No. fmcp-23-111300 (Q), **Revised:** 20 September, 2023, Manuscript No. fmcp-23-111300 (R), **Published:** 25 September, 2023, DOI. 10.4172 fmcp.2023.20(4).

as a means of achieving optimization (e.g., through automation of clinical workflow) and more radical transformation (e.g., virtualization of care delivery or the use of AI to diagnose and adjust treatment plans largely without clinical intervention).While the Hospital should provide the Healthcare services in order to serving people well. For this reason, the need for Cyber Security standards is recurrent since every year thousands of people died as the result of clinical errors caused by fatigue or inaccuracy that could have been prevented with proper technology [3]. Most of the problem shave to do with lack of coordination between systems due to the use of different standards [4]. Anybody waiting for the standards bodies before implementing Cyber Security standard will be waiting such long time, but information security must stay manageable and able to let preventing threats, reduce vulnerabilities and risks. Those endpoints are even more important since the clinical images can be used for ANN (Artificial Neural Network) applications and data can be used for Deep Learning and Big Data algorithms developments with all the implications that Data Management has in an Artificial Intelligence System [5,6].

■ Cyber security framework in the healthcare environment

Organizations have realized that some of these frameworks that are successful in other sectors do not fully address healthcare specific concerns. Due to the lack of prescriptiveness of some of these frameworks, organizations have not been able to adapt the principles, standards, guidelines, and best practices from the framework to their specific context and develop practices that meet their own needs. The use of standards can be viewed from legal and IT architecture perspectives [7]. From the legal perspective, there are ranges of standards that either recommends general or specific scenarios in healthcare, as General Data Protection Regulation (GDPR). From IT standards perspective, we refer a range of Cyber Security standards to assist in the development of security plans and mitigate risks. However, this has resulted in an assorted range of standards being developed for specific instances of technology use, as: International Organization for Standardization (ISO)/IEC 27799, Health Insurance Portability and Accountability Act (HIPAA), HITRUST, Nation Institute of Standards and Technology (NIST) has developed the Cyber Security Framework (CSF) and GDPR. Many standards do not include sufficient security-related provision and given the complex nature of standards, it has resulted in many providers selling security management solutions for interpretation of the standards and also to explore its implementation.

■ ISO27799

ISO/IEC 27001published by International Organization for Standardization (ISO) is a collection of Information security management best practices and provides requirements for Information Security Management Systems (ISMS). The standard was published in 2005 and revised in 2013. While the ISO 27799 applies ISO/IEC 27002 to the healthcare domain in a way that carefully considers the appropriate application of security controls for the purposes of protecting personal health information. ISO 27799 therefore places constraints upon the application of certain security controls specified in ISO/IEC 27002. It also enables organizations to verify that risks are properly identified and managed. To provide security controls to protect Personal health information.

Organizations can voluntarily choose to adoptISO27799 and can become ISO27799 certified. This involves an initial audit and subsequent follow-up compliance audit to maintain the certification. The certification audit scope and requirement include a complete assessment of information security best practices applied to an organization.

■ HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is one of the biggest drivers for organizations to protect electronic Protected Health Information (ePHI) against threats and hazards. HIPAA defines the security rule that requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. Due to HIPAA's high-level nature of the requirements which are not being prescriptive, along with the absence of a complete risk analysis with just over-reliance on implementing various safeguards, the information protection programs across various organizations incorporating HIPAA have varied. Without valid risk analysis and just complying with HIPAA security rule would result in an approach that does not handle all the threats that a healthcare organization is prone to Compliance with HIPAA requires organizations to either verbally commit to their customers or sign agreements to demonstrate compliance. In addition, organizations will also be required to provide compliance or attestation reports to prove compliance.

■ HITRUST

HITRUST was formed by a consortium of healthcare organizations in 2007 with aim of making information protection a core pillar of healthcare information systems and exchange. Developed by taking inputs from various healthcare and information security leaders. The HITRUST framework aims to meet the organization's needs of providing specific guidance on the application of the framework to the healthcare sector. As per HITRUST, the programs include the establishment of a common risk and compliance management framework (CSF); an assessment and assurance methodology; educational and career development; advocacy and awareness; and a federally recognized cyber–Information Sharing and Analysis Organization (ISAO) and supporting initiatives. Includes various typical information protection area like access control, privacy as defined in ISO27799. HITRUST is a certifiable framework that organizations can use for the creation, storage, and exchange of personal health information. The certification process involves two-steps. Organizations first need to initially perform a self-assessment using a tool provided by HITRUST. Based on inputs provided to the tools, a customized assessment is created to assess the organization's environment with respect to the compliance criteria.

■ NIST CSF

To address the ever-increasing attacks on critical infrastructure, Nation Institute of Standards and Technology (NIST) has developed the Cyber Security Framework (CSF) that provides an incident management-based model that various sectors or organizations can leverage for improving the management of cybersecurity risk. The NIST CSF framework is built on the foundations of threat modeling, threat intelligence, and collaboration. Leveraging such a framework helps organizations perform proper risk analysis, proactively address active and emerging threats, and collaborate with various entities to effectively address cyber threats. The framework is not certifiable. However, an audit of the security controls that are aligned with NIST CSF can be performed as part of ISO27799 audit report.

■ GDPR

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

Controllers of personal data must put in place appropriate technical and organizational measures to implement the data protection principles. Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data and use the highest-possible privacy settings by default, so that the datasets are not publicly available without explicit, informed consent, and cannot be used to identify a subject without additional information.

Healthcare organizations are in a vital position as they handle an entire spectrum of data, from financial records and health insurance information to patient test results and biometric information. Some of these data types are more sensitive than the typical information collected by non-healthcare organizations.

Apart from the general protections provided for personal data, the GDPR also defines three types of "health data" that require special protection: data concerning health, genetic data, and biometric data. These are classified as sensitive personal data, and the regulation generally prohibits any kind of processing for these unless explicit consent is given, or very specific conditions are met. Compliance with GDPR requires organizations to define (article 37) a Data Protection Officer (DPO) a person with expert knowledge of data protection law and practices—must be designated to assist the controller or processor in monitoring their internal compliance with the Regulation.

Adoption of Cyber Security Framework

It is clear that healthcare is one of the most complex businesses with a large diversity of types of interactions [8-9].The possibility of using IS and Security Standard to support the services delivery also opens new opportunities. Smith has proposed that only Information Systems (IS) could bridge the information "chasm", while the Security Standard could reduce the risk to leak the data [10].

To address the healthcare-specific needs various frameworks are available for organizations to choose from. Our framework will be based on various parameters like Comprehensive general Security, Prescriptive, Supported and Maintained, Practical and Scalable, Audit or Assessment guidelines, Certifiable, Open Standard, Cost of Certification, Report, Creation a value for Organization.

Based on our experience, there are only two standards that combined together could cover all Cyber Security aspects, they are: ISO 27799 [11], and GDPR **(TABLES 1, 2)** [12].

To take advantage of an IS and Security Standards it is necessary a leadership to promote the alignment of business with them. In this complex environment the role of the Chief Information Officer (CIO) or Chief Information Security Officer (CISO) is critical to ensure good focus on organizational specificities. It was recognized that best performing Health departments were related with department heads that matched CIO/CISO attributes, like openness to suggestions and excellent relationship with other healthcare professionals; leadership skills, which help them to address challenges; meaningful negotiation skills which are used in their relationships with the vendors, openness to bolder projects with new technologies, etc.

Future Research Plan

Conceivably the implementation of these Cyber Security Framework will be done by different

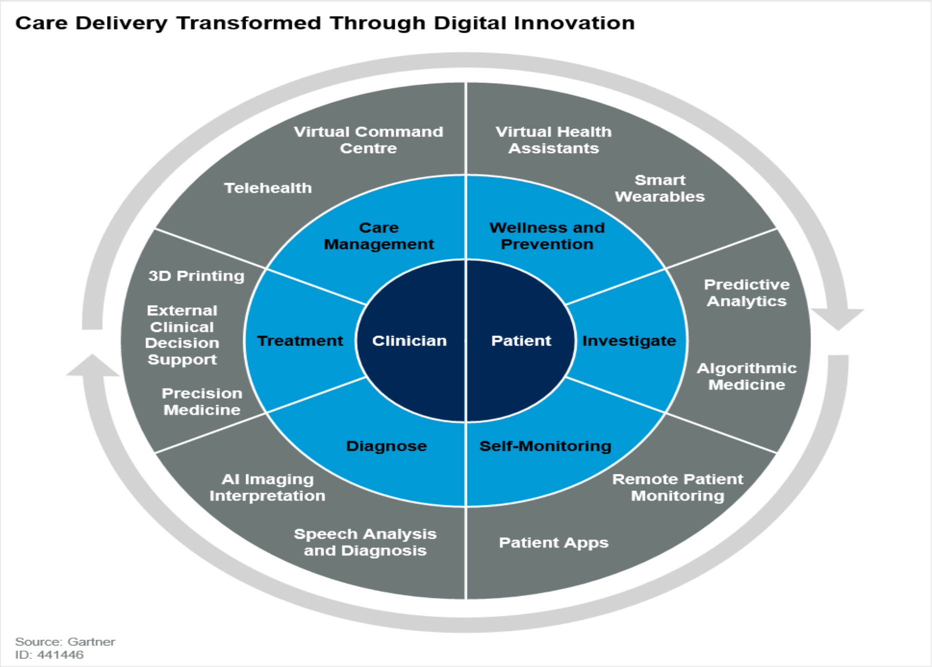
TABLE 1. Summarize the various parameters organizations need to consider while selecting the framework.

Requirement	HITRUST	ISO27001	NIST CSF	HIPAA	GDPR
Comprehensive general Security	Yes	Yes	Yes	Partial	Yes
Prescriptive	Yes	Yes	Partial	No	Yes
Supported and Maintained	Yes	Yes	Yes	No	Yes
Practical and Scalable	Yes	No	No	Yes	Yes
Audit or Assessment guidelines	Yes	Yes	Yes	No	Partial
Certifiable	Yes	Yes	No	No	No
Open Standard	Yes	No	Yes	Yes	No
Cost of Certification	15K USD	100K USD	No	No	No
Report	Yes	Yes	Partial	No	Partial
Creation a value for Organization	No	Yes	No	No	Yes

TABLE 2. Show the main areas covered by these standards and how these areas are covered

Area	ISO27799	GDPR
Information security policies	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations	To provide at TOP management a direction for data management in term of privacy
Organization of information security	To establish a management framework to initiate and control the implementation and operation of information security within the organization	To establish a Data Protection Office (DPO) in order to manage the implementation of Data Privacy
Human resource security	To ensure that employees and contractors understand their responsibilities and are suitable for the roles in term of CyberSecurity for which they are considered	To ensure the employees and contractors understand their responsibilities in term of Privacy and how handle the data
Asset management	To identify organizational assets and define appropriate protection responsibilities	Give general guideline to identify organizational assets
Access control	To limit access to information and information processing facilities.	Give general guideline to manage access control. This aspect are covered by other local law
Cryptography	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of informat	It defines the concept of pseudonymisation, in which in a particular personal case, this data must be anonymized so that the data itself can no longer be directly and automatically attributed to a specific interested party. Suggest also in some cases to use the Cryptographic algorithms
Physical and environmental security	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities	No Covered
Operations security	To ensure correct and secure operations of information processing facilities	To provide a general definition about kind of data and how handle it
Communications security	To ensure the protection of information in networks and its supporting information processing facilities	To define how exchange the information with any external entities

System acquisition, development and maintenance	To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks	No Covered
Supplier relationships	To ensure protection of the organization's assets that is accessible by suppliers	To define how exchange the information with any external entities and supplier’s role
Information security incident management	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses	To define the creation of a Data breach register in order to record all incidents regarding personal data
Information security aspects of business continuity management	To ensure proper and effective use of business continuity management systems.	Give general guideline to manage a disaster recovery plan
Compliance	Give general guideline in health sector in term of objectives of the analysis and the possibility of unexpected findings Example of Law is : Council of Europe Recommendation, R (97)5 On the Protection of Medical Data, Council of Europe, Strasbourg, 12 February 1997	Includes penalties in case of non-compliance with the law


Care Delivery Transformed Through Digital Innovation

Source: Gartner
ID: 441446

FIGURE 1. Care delivery transformed through digital innovation.

departments in health service organizations if they should choose to implement this management system standards. This will be economically unreasonable particularly since an increasing overlap appears to be developing between management system standards as well as more focus on creating Integrated Cyber Security Framework.

Currently, Health Organization are impacted from innovation waves as: AI in healthcare, algorithmic medicine, diagnostic image interpretation and automated imaging workflow. The use of natural language processing during the clinical encounter will be used to detect behavioral health conditions and for automated accurate clinical documentation. All these items have an impact on Cyber Security aspects **(FIGURE 1)**.

It is important also to consider:

- Integration with ERPs that represent the full care record across organizational boundaries are maturing with many regions now working on Health Information Exchange and addressing semantic interoperability gaps. These solutions expose clinical records to the patient on a device of their choice and facilitate patient scheduling and other convenient transactions.
- Precision medicine and health, including genomic medicine, enable targeted treatment and improved medical knowledge alignment to situations.

- How the Virtual care platforms support timely clinical encounters and remote patient monitoring. This is breaking physical constraints of the care facility while making care more convenient and scalable.

Discussion & Conclusion

The purpose of this research was to determine the best Security Standards to use and compare them to define a correct Cyber Security Framework. Based on our analysis the ISO27799 family's standard provides right additional directives that are covered in part from GDPR and this combination is the best. In conclusion using Security Standards are essential to ensure the delivery of benefits to the patient and healthcare providers in information interoperability. This is only part of a bigger effort to implement a comprehensive strategy that allows consistency of information collection and sharing within the healthcare sector. The CIO/CISO role and understanding of the organization's environment is key to deliver real interoperability potential to the organization to patients' benefit.

Declarations

■ Ethics approval and consent to participate

This study followed the ethical principles of the Declaration of Helsinki. Participation in the study was voluntary. Before inclusion in the study, clinical staff explained the purpose of the study and informed consent form was secured from each participant.

■ Consent for publication

We have had authorization for publication like our Hospital Privacy Policy already require.

■ Availability of data and materials

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

■ Competing interests

The authors declare that they have no competing interests.

Funding

This article did not receive sponsorship for publication.

Acknowledgments

Campania Regional Council to support the Project development.

References

1. Healthcare Innovation Trends: Transforming Care Delivery – Gartner October (2019).

2. Cyber Security Framework for Healthcare - Kiran Gurudutt – March (2018).

3. Thompson T. US Former secretary of Health and Human Services Keynote Speech at the 2007 CDHC Expo. Business Wire. 13, (2006).

4. Bell K. "HIT and Pay for Performance". Acting Deputy, US Office of the National Coordinator for Health Information Technology Keynote Speech at the HIT Symposium at MIT. 17, (2006).

5. Parmeggiani D, Avenia N, Sanguinetti A. et al. Artificial intelligenceagainst breast cancer (A.N.N.E.S-B.C.-Project). *AnnItalChir*. 83, 1-5 (2012).

6. Piantadosi, G, Bovenzi, G, Argenziano, G et al. Skin Lesions Classification: A Radiomics Approach with Deep CNN. *Springer Int. Publ.* 11808, 252-259 (2019).

7. Bollino R, Bovenzi G, Cipolletta F et al. "Synergy-Net: Artificial Intelligence at the Service of Oncological Prevention." *Intell Syst Ref Libr.* 211, 389–424 (2022).

8. Plsek P and Wilson T. Complexity, leadership, and management in healthcare organisations. *Bmj*. 323, 746-749 (2001).

9. Lapão LV. Survey on the status of the hospital information systems in Portugal. *Methods Inf. Med.*46, 493-499(2007).

10. Smith R. The future of healthcare systems: Information technology and consumerism will transform health care worldwide. *Bmj*. 314, 1495 (1997).

11. ISO/IEC 27799:2016Healthinformatics — Information security management in healthusing ISO/IEC 27002.

12. 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, and repealing Directive 95/46/EC (General Data Protection Regulation). *Off. J. Eur. Union*.