2021 43rd Annual International Conference of the
IEEE Engineering in Medicine & Biology Society (EMBC)
Oct 31 - Nov 4, 2021. Virtual Conference

PANACEA resilient and secure toolkit for healthcare infrastructures

Stelios Sfakianakis, Emmanouil G. Spanakis, Pasquale Mari, Ivan Tesfai Ogbu, Martina Bossini Baroggi, Sabina Magalini and Vangelis Sakkalis

Abstract— **Healthcare organizations are frequently subject to cybersecurity incidents. The outbreak of a pandemic such as COVID-19 has shown the need for specific operational and organizational measures to be in place in order to reduce the risk of successful cyberattacks. Time will be key: preparation is needed to ensure quick secure set-up of additional resources (IT, staff, medical devices) when the next emergency will hit. The PANACEA Solution Toolkit is a suite of complementary tools to provide Health Care Organizations (HCO) with assessment, guidance, technical and organizational "infrastructure" to address the cybersecurity challenges. It provides support for fortifying health organizations against cyber threats on multiple different levels (technical, behavioral, organizational, strategical) and across a diverse set of workflows and scenarios. In order to determine whether the toolkit satisfies the specific business and users' requirements in the selected use cases, a detailed validation plan and execution roadmap is established taking into account the constraints of the current emergent situation.**

I. Introduction

Healthcare institutions today seem to be an attractive target for cybercrimes [1]. Two fundamental reasons sustain this reality: healthcare is a rich source of valuable data and its defenses are proven to be weak. The reason for this weakness can be further attributed to the complexity and dynamism: a multiplicity of connected end-points (including devices and mobile consumer devices whose number and type can change on a day-by-day basis), many different interconnected systems (including no more supported legacy systems [2]), and digitalization of patient data. A recent survey conducted in the USA shows that, even if 94% of the respondents use advanced technologies for sensitive data, 60% do not adopt appropriate data protection measures, mainly because of complexity (53%), skill shortage (39%), performance concerns (36%), lack of budget (33%), and lastly lack of organizational buy-in (26%) [3]. This increasing risk of cyber-attacks, both from inside the infrastructure or from outside, either intentionally or not, can have a huge impact in these critical infrastructures. A recent report [4] shows that threats based on human errors are perceived to have the highest likelihood of occurrence and are rated as the second most "critical" threat in terms of impact on Hospital operations (70% of the respondents said that it is critical). More than that today, innovative medical IoT devices and healthcare services can improve care, empower patients and maximize efficiency, but cybercriminals target their vulnerabilities [5].

On 11th of March 2020 WHO declared COVID-19 as a pandemic after a global outbreak of incidents. This alerted healthcare authorities and all available resources were used in order to compensate the negative effects of the disease. Today, we are still facing an unprecedented and unexpected global public social and health crisis. From the early beginning ICT became the epicenter and was used as means of compensations to allow continuation of daily activities. Healthcare was forced to utilize new tele-care pathways aiming to enable the continuation of care by improving risk-adjusted patient outcomes [6], utilize hospital resource and infrastructures, promote patient safety, and also predict pandemic outbursts to allow authorities to engage appropriate measures on time and with high possibility of success [7]. This rapid mitigation and transformation of healthcare towards digitization increased the attack surface, cybersecurity threats and risks space and performance issues due to significantly increased workload, and became a threat to business continuity [8]. Recently published literature identified methods to fill the gap of increasing demand of use of resources and propose new innovative schemes that could be effectively applied in healthcare and avoid the underlined costs of their adverse effects [9]. It seemed like COVID-19 was an opportunity to extent attacks for financial gains and promote cybercrime, and the work of Khan et all observes ten important such threats during the period of COVID pandemic [10]. In [11] a number of IT risk and resilient aspects were presented in order to allow further developments, explore, plan, strategize, and show ways to act, including healthcare organizations. The authors of [12] studied why these cyberattacks have been predominantly problematic during COVID-19 and ways that health care industries can better protect patient data. The work in [13] outlines key cyber-security principles for healthcare organizations and also academic institutions related to this pandemic and on the ways, they affected and will affect healthcare delivery, noting that there is a clear need to strengthen frontline medical services that are neglected in terms of security.

Thus today, treating patients is not the only concern healthcare is facing. Healthcare systems must also adjust their operational requirements to face cybersecurity

* This work has been supported by PANACEA project that has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement no 826293 and Daphne that received funding from the Hellenic Foundation for Research and Innovation (HFRI) and the General Secretariat for Research and Technology (GSRT), under grant agreement No 1337.

Stelios Sfakianakis, Emmanouil G. Spanakis and Vangelis Sakkalis are with the Computational Biomedicine Laboratory, Institute of Computer Science, Foundation for Research and Technology – Hellas, Heraklion, Crete, Greece; e-mail: {ssfak, spanakis, sakkalis}@ics.forth.gr). (Corresponding author: Stelios Sfakianakis, phone: +30-2810-391650).

Pasquale Mari and Sabina Magalini are with the Fondazione Policlinico Universitario Agostino Gemelli, Roma, Italy, (email: pasqualemari3 @gmail.com, sabina.magalini@unicatt.it)

Ivan Tesfai Ogbu and Martina Bossini Baroggi is with RINA, Holding Company RINA S.p.A., Via Gran S. Bernardo, MILAN, Italy (email: {ivan.tesfai, martina.bossini}@rina.org)

challenges. In that respect, PANACEA aims to create and validate these needed *tools for cyber security assessment and preparedness of Healthcare ICT infrastructures and connected devices [14]. PANACEA proposed two such tools, the Solution and the Delivery Toolkits* [14]. The Solution Toolkit will positively affect the cybersecurity of a Health Care Organization (HCO) according to a holistic modality, assessing (and acting on) the physical, software and organizational/human components of the HCO, relevant for the cybersecurity. The Solution Toolkit also manages the connections with other HCCs, even when this HCCs are not adopting. The Delivery Toolkit is conceived as a support for the adoption of the Solution Toolkit. It involves two support tools: a methodology to evaluate the return of investment of cybersecurity interventions and a set of adoption guidelines.

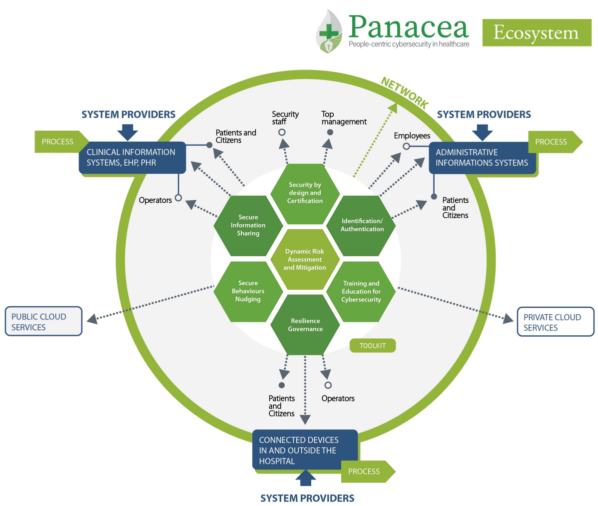

Figure 1: PANACEA Solution and its interactions with the healthcare ecosystem

The PANACEA Toolkit is expected to be used for prevention purposes to proactively protect HCC IT infrastructure. Our goal in this paper is to describe the integration "capacity" of the Toolkit in the generic heath care ecosystem, which includes the healthcare organizations, the various stakeholders, focusing on the increased needs for cybersecurity in the context of a pandemic such as COVID-19. We also present the validation plan and relevant activities and define methods and KPIs to validate the integrated use of PANACEA tools and verify its integration capability. In the following sections we present PANACEA Solution Toolkit, its integrated configuration capabilities, how it addresses multitude of healthcare cybersecurity needs, validation methodology in the COVID-19 period, when the access to HCO non-clinical activities is limited.

II. PANACEA Toolkit

The PANACEA Solution Toolkit is a suite of complementary tools to provide a HCO with assessment, guidance, technical and organizational "infrastructure" to address cybersecurity challenges. The Solution Toolkit is built as a collection of tools, each of which aims at a specific area of cyber risks both at the technical and the organizational and human fronts (Figure 1, a generic view of the interaction within its operational environment). From its initial inception the Solution toolkit has been defined to contain four technological tools:

- a dynamic risk assessment & mitigation tool (Dynamic Risk Management Platform, DRMP), helping to perform risk assessment evaluation and mitigation measures,
- a secure information sharing tool for the secure transfer and sharing of sensitive health data (Secure Information Sharing Platform, SISP)
- a security-by-design & certification framework (Security by Design Framework, SbDF) that is further split into the Secure Design Support Platform (SDSP) and Compliance Support Tool (CST), which together facilitate the design of new systems based on established standards and best practices and check the compliance with them
- the Identity Management Platform (IMP) which supports the identification & authentication of users and systems in a variety of scenarios covering both human to machine (H2M) and machine to machine (M2M) communication

It additionally contains the following "organizational" tools:

- a tool composed by models, guidelines and best practices for training & education (Training & Education for Cybersecurity Tool, TECT)
- a tool aimed at resilience governance (Resilience Governance Tool, RGT) including guidelines for cybersecurity distributed organizational model and a compliance control list
- a tool for secure behaviours "nudging" (Secure Behaviour Nudging Tool, SBNT) to provide behaviour-change interventions relevant for cyber security.

The tools (hexagons in Figure 1) can be used separately, deployed and managed by the personnel and the actors of an organization. The tools operate on an "ecosystem" made up of a variety of components of an HCO: network, information systems, devices (inside and outside the HCO), operators (medical doctors, nurses), administrative and technical staff, patients/citizens. In view of the above, our main objective is to elaborate the integration aspects of the Toolkit and its deployment, role, and use in the healthcare ecosystem.

III. PANACEA Toolkit Integrated Configuration

We identify different aspects of integration: *internal* integration addressing the relationships and interdependencies of the individual tools; and *external* integration, which deals with the toolkit's role in the clinical context, the way it interacts and positively "*disrupts*" the cybersecurity policies, processes, and techniques of its operational environment. Using these notions, in this work we study how the individual tools can be used together and what are the guidelines for using them as a whole in the clinical context. Through the refinement of the internal and external integration features of the Toolkit, we identify the following cases, shown as layers in Figure 2:

- Integration "into" the HCO, tool specific integration guidelines and deployment inside the operational environment of an Organization (people, systems, and processes);
- Integration "within" the Toolkit, addresses the interactions and collaborations between the different tools of the Solution Toolkit;

- Integration "across" the HCO, deals with the coordinated use of the Toolkit in order to support pervasive and overarching processes in the Organization;

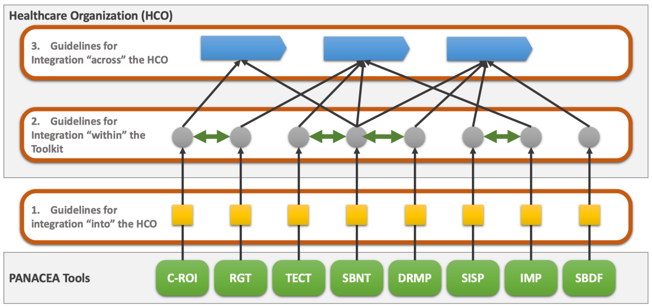

Figure 2 3-layered view on the integration of the Solution Toolkit

As we move between the different layers, we extend the scope of integration from the most specific (bottom) to the most general (top). Starting at the bottom layer, integration "into" the HCO is the most basic one and most relevant for the owner/developer of an individual tool. Going upper, integration "within" a HCO requires the cooperation of different tools and respective tool developers, while at the top layer integration "across" the HCO is the orchestrated use of the whole Toolkit where not only the owners of the tools but also the HCO managers, policy makers, and administrators need to be involved. At this level of integration, the Solution Toolkit will have more "disruptive" effects on the HCO, for example requiring people or groups of people to change their work processes and behaviors to effectively implement the proposed cybersecurity changes. The inclusion of the C-ROI tool ("Cyber – Return On Investment") in the figure, which relates to guidelines for the financial viability of cybersecurity measures in HCO and is part of the Delivery Toolkit, aims to convey this idea that in the most general "across" case, a more holistic evaluation and deployment of the Toolkit is necessary by prioritizing cybersecurity investments based on their impact and cost.

At each different layer specific guidelines to achieve the specific level of integration are needed. In order for a PANACEA tool to be integrated into a HCO, multiple aspects need to be considered, such as the technical and organizational requirements, the cyber defenses to be addressed, and the use cases and their implementation to be supported. Using parts of the Toolkit can maximize the added value, i.e. for the secure management of users' identity during the sharing of clinical information, the consolidation of "nudging interventions with training, etc. At the third layer, the Toolkit can provide HCOs with facilities for the cybersecurity certification and compliance with established standards, and support more high-level reference use cases. In the following we focus on the integration "across" the HCO for the handling of an emergent situation like COVID.

IV. Integration "across" an HCO to cope with "structural" and COVID like situations

The PANACEA Solution Toolkit is posited to greatly facilitate the compliance of a HCO with established standards and to cope with COVID-like situation, when resilience is key. We identify the following needs.

A. *"Structural" healthcare needs*

There is an "operational" dynamism: in a hospital there is a multiplicity of connected end-points, whose number and type can change on a day-by-day basis. And there is a "structural" dynamism: digitization is growing and a positive side-effect of COVID in Europe is that it has surfaced the weaknesses of the national health services and the need to invest in e-health and tele-health. ICT investments are expected to increase [15]. From the cybersecurity point of view, this is an opportunity. Systems and interconnected medical devices are becoming more and more mission-critical, but are still poorly protected and vulnerable. A reason is that most of the existing assets were designed when data privacy and cybersecurity were not an issue. Investments in new systems and interconnected medical devices allow to radically improve this, if a "Security by Design" approach is adopted. Also, healthcare working environment has many characteristics that make human behaviour a cybersecurity hazard and its change problematic [16]. Work culture can lead to security being overlooked or perceived as a burden, particularly if it is perceived to detract from patient care. Working environment is also prone to regular changes to team structure through rotation of staff members and new intakes. Finally, *EU Directive 2016/1148* describes the measures for a high common level of security of network and information systems across EU. Its scope are the operators of essential services including health care settings [16]. Each European member state complies with the Directive and makes it operational, also through control lists to assess their "maturity" with regard to cybersecurity. As a consequence, the operators are expected to do investments to fill the gaps.

B. *COVID-19 related needs*

We describe below how the use of PANACEA toolkit can support an HCO needs through the integrated use of two or more tools.

TABLE I. Contributions of PANACEA in Covid-like context

DRMP	Simulate rapidly new types of attack and automatically provides remediation actions, ranked by priority
SISP	Allow the fast activation and use of a secure clinical data and image sharing mechanism based on "ready-to-use" federation agreements and protocols
IMP	Use of password + face identification (through employee's smartphone) to access both workstations and medical devices
SbDF	Ensure through a "secure software design check-list" that the design process and its "product" (e.g. an new App, a new certified diagnostic device, a new networked system) are secure
SBNT	Rapidly identify, design and deploy "nudges" to get secure behaviours from "old" and "new" staff (e.g. Posters, Memes, Screensaver messages) specific to the crisis at hand
TECT	Include e-self-learning and remote training delivery solutions, quite suitable in a crisis where face-to-face interaction is not possible and "mass training" is needed in short time
RGT	Ensure fast development and diffusion of policies specific to the crisis at hand inlcluding information security experts and reference persons operation within / without a HCO

We have identified and analysed a number of different use cases where parts of the Solution Toolkit can address critical cybersecurity challenges in both structural and COVID-like situations (Figure 3).

Use cases		PANACEA "Solution Toolkit"						
Source	Short description of the needs to be satisfied using the tools	DRMP	SISP	SbDF	IMP	SBNT	TECT	RGT+ C-ROI
Healthcare specificities	1. To cope with frequent selection and deployment of new technology	x		x	x	x	x	x
	2. To limit human errors due to multi-use and time pressure	x	x		x	x	x	x
EU Directive	3. To decide cybersecurity investments	x				x		x
Covid-19	4. To contrast stream of fake pandemic related messages					x	x	x
	5. To ensure secure Smart-working	x	x	x		x	x	x
	6. To ensure secure rapid on-boarding of new staff in clinical activities				x	x	x	x
	7. To ensure secure Telemedicine	x	x	x	x		x	x
	8. To ensure secure upgrade to sanitary purposes of non-sanitary host structures	x	x	x	x	x	x	x

Figure 3: Use cases and associated PANACEA tools

As an example, here we present how PANACEA supports the need for secure telemedicine during the COVID-19 pandemic (use case 7). *Problem and use case:* In case of COVID-like emergency, the policy is to keep non-severe COVID patients at home, there's need for telemonitoring and increased use of telemedicine that has low level of security. The use case regards the activation of a telemedicine service where the combined use of six PANACEA tools allows to apply a "security by design" approach to minimize the risk introduced by the connection and by the remote operation by patients and local assistance staff. *Target context.* Patient's home and HCO department taking care of them; Telemedicine system; Tools, activity flow and responsibilities. Figure 4 below presents the series of steps, the tools, and the actors participating with their roles.

Activity	Flow	Tool	CISO	DPO	ICT	Clin Eng	HR	ISRP	HCO Staff	Patients/ Home Assist	Task Force
Set-up Task Force	1	RGT	A/R	C	C	C	C				
Identify target patients/home assistants & operating context	2								C		A/R
Estimate risk profile of target patients and home assistants	3	SBNT	C	C	C	C	A/R	C	C	C	
Identify technical security issues and mitigation actions	4	DRMP/ SbDF	A/R	C	C	C	C				
Design tech. mitig. measures, including SISP (if needed)	5	(SISP)	I		A/R						
Design and implement Video Clips	6	TECT	C	C	C	C	A/R	C			
Launch Telemedicine risk mitigation initiative	7										A/R
Deploy. tech. mitig. measures, train on SISP (if needed)	8	(SISP)	I		A/R					I	
Diffuse Vdeo Clips to reach target	9	TECT					A/R	I		I	
Monitor impact on behaviours	10	TECT	C	C	C	C	A/R	C	C		
Analyse and take action if needed	11							C			A/R

Figure 4: Ensure secure Telemedicine services during a pandemic – activities, actors, and roles (R=Responsible; A=Accountable; C=Consulted/Contributor; and I=Informed)

V. Validation Methodology

This section describes the overall validation methodology that was followed aiming to determine whether the final product satisfies the specific business and users' fundamental requirements within its intended environment. During the development phase, verification was performed in parallel with system definition and realization. Then, validation is applied focussing on three crucial aspects: mapping between user requirements [18] and use cases, collection of information from end-users in order to define the baseline, and tests to assess key performance indicators and trace user requirements coverage.

PANACEA's solution toolkit validation aimed to ensure that all building blocks were assessed in relation to their compliance with each specific purpose and function. Figure 5 shows the validation workflow activities. In particular, the organizational contexts in which the tools are validated refers to the situations offered by the end-user organizations taking part to the PANACEA project; user scenarios and the related use cases allow to validate the capability of the tools to improve the protection of the organizations in the attack, behaviour and regulatory scenarios; tools were developed to fulfil the technical requirements, which refer to the user requirements and to the expected innovations; therefore, the use cases referring to a tool allow to validate the tool with respect the related user requirements and each use case refers to a tool, the Key Performance Indicators (KPIs) related to a tool will be measured for each use case.

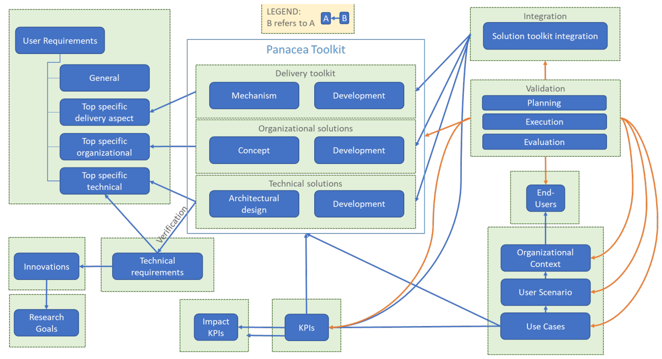

Figure 5: PANACEA Validation Context Workflow

These indicators will provide quantifiable means for measuring the positive impact of the PANACEA toolkit into the selected scenarios. A KPI elicitation based on the "with/without PANACEA" concept was introduced representing current realization of scenarios in the relevant organizational contexts. The benefits of this approach are that it allows to perform *differential* analysis, i.e. to compute the "delta" between with and without KPIs values, in order to calculate the added value, and to enable traceability among user requirements and provide a direct validation of the toolkit with respect to user needs.

An instrumental report template has been used to define and associate use cases, KPIs, user requirements and information on how to assess the solution toolkit performance. It allowed to structure the information provided, which led to the definition of *41 validation tests grouped by use cases*. Each test outlines the following information: KPIs and user requirements covered by the test, participants, objectives, training information, steps for execution and result data to be collected. After defining the tests, a traceability matrix was extracted to better manage and trace user requirements coverage against validation tests. These 41 tests, performed during the execution phase by the end user in each user scenario, allow us to compute with and without KPIs values for the differential analysis. For each use case, a six-week period was arranged to comprise training (1 week before all execution activities) and execution of test for "without" (2 weeks) and "with" case (2 weeks). Finally, the aspect of risk management of the validation activities was addressed with eleven risk categories identified and associated with PANACEA tools. The most relevant risks were related to user's participation, maturity and stakeholder role diversity and are presented in Figure 6 below.

RISK	DRMP	IMP H2M	IMP M2M	SISP	SbDF	SBNT	TECT	RGT
User participation/staff		x	x	x		x	x	
User participation/manager								x
User participation/cybersecurity professionals	x				x	x	x	x
User Maturity/ Internal User	x				x	x	x	x
User Maturity/ external stakeholder		x	x	x	x	x	x	x
Feedback Bias	x				x			x
Stakeholder role diversity	x	x	x	x	x	x	x	x
Statistical significance (of the sample of use case instances):								
depends on sample size of [user]		x				x	x	
depends on sample size of [situation]		x				x	x	
depends on sample mix of [user]		x				x	x	
depends on sample mix of [situation]	x	x			x	x	x	

Figure 6: Risks for each PANACEA tool

Then risks were correlated with KPI to measure importance and propose possible mitigation actions. The most recurrent mitigation actions were: timely identification of the test personnel involved in the validation and perform appropriate communication via direct supervisors and relevant management; clear definition of stakeholder's roles to check and monitor satisfying coverage of multi-stakeholder perspective; training the professionals on use of the PANACEA tools and how the adoption can contribute to their duties. A focus analysis was performed and identified the following factors that can be obstructed by COVID-19: on site presence of tool owner, needed for set-up, monitoring; on site presence of MD Manufacturer originally needed; IT professionals involved; Clinical Engineering professionals involved; HR/Training professionals involved; clinical, administrative and management staff involved. After these factors were associated with use cases led to the identification of the mitigation actions for each PANACEA tool (i.e., use of ICT to overcome extra-ordinary organizational barriers and allocate available resources).

VI. Conclusion

In today's highly digitalized world, there's an emergent need to secure healthcare organizations and their assets, and especially the most critical asset which is the patients' themselves and their health-related information. This is further amplified by the rate of "change" introduced even in traditionally conservative environments such as HCOs with the adoption of new techniques, technologies, business scenarios and requirements (e.g., health information sharing [19]). Health IT solutions used in clinical practice have the largest impact and therefore cybersecurity solutions need to be in place for the benefit of the patients, as well as the health business entities and other stakeholders [20]. Addressing cyberthreats, especially in the extraordinary circumstances of a pandemics outbreak, requires a multifaceted response strategy that involves not only technical solutions, but also affects user training and behavior monitoring, business processes, and governance.

In this work we have presented PANACEA, that provides a comprehensive set of tools to address these challenges. In particular we have argued that the: integrated use of technical and non-technical tools, allows HCOs to cope with many cybersecurity challenges structurally specific to the healthcare sector better than using only technical or non-technical tools; a HCO that has already adopted PANACEA framework today is capable to rapidly set-up measures for coping with the cybersecurity risks generated by a COVID-like situation; and that all the above can be validated with our proposed methodology, operable also under COVID operational limitations. The validation activities are currently in progress in three HCOs (in Greece, Ireland and Italy) and related results will be available by end 2021.

References

[1] Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Journal of medical Internet research, 20(5), e10059. doi.org/10.2196/10059

[2] National Audit Office, Investigation: WannaCry cyber-attack and the NHS, 2017.

[3] Thales, Trends in Encryption and Data Security: Data Threat Report-Healthcare edition, 2017

[4] ENISA, Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures, 2016

[5] T. Webb and S. Dayal, "Building the wall: Addressing cybersecurity risks in medical devices in the USA and Australia" Computer Law & Security Review, 33(4), 559-563, doi.org/10.1016/j.clsr.2017.05.004.

[6] R. Ohannessian, T. A. Duong, and A. Odone, "Global Telemedicine Implementation and Integration Within Health Systems to Fight the COVID-19 Pandemic: A Call to Action," JMIR Public Health Surveill, vol. 6, no. 2, p. e18810, Apr. 2020, doi: 10.2196/18810.

[7] M. Spanakis, M. Zoumpoulakis, A. E. Patelarou, E. Patelarou, and N. Tzanakis, "COVID-19 epidemic: Comparison of three European countries with different outcome using Gompertz function method", Pneumon 2020, 33(2):1-6 http://www.pneumon.org/arpil-june-2020-vol-33-issue-2/newsid789/780

[8] Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. SA Journal of Information Management, 23(1), 11 pages. doi.org/10.4102/sajim.v23i1.1277

[9] Williams CM, Chaturvedi R, Chakravarthy K Cybersecurity Risks in a Pandemic J Med Internet Res 2020;22(9):e23692 doi: 10.2196/23692PMID: 32897869PMCID: 7528623

[10] Khan, Navid Ali; Brohi, Sarfraz Nawaz; Zaman, Noor (2020): Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.12278792.v1

[11] T. Weil and S. Murugesan, "IT Risk and Resilience—Cybersecurity Response to COVID-19," in IT Professional, vol. 22, no. 3, pp. 4-10, 1 May-June 2020, doi: 10.1109/MITP.2020.2988330.

[12] Williams CM, Chaturvedi R, Chakravarthy K Cybersecurity Risks in a Pandemic J Med Internet Res 2020;22(9):e23692 doi: 10.2196/23692PMID: 32897869PMCID: 7528623.

[13] Menaka Muthuppalaniappan, LLB, Kerrie Stevenson, MBChB BMedSci (Hons) FHEA, Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health, International Journal for Quality in Health Care, 33(1), 2021, doi.org/10.1093/intqhc/mzaa117

[14] https://panacearesearch.eu/

[15] https://www.idc.com/getdoc.jsp?containerId=EUR146245720

[16] D. Branley-Bell, et. al, "Your hospital needs you: Eliciting positive cybersecurity behaviours from healthcare staff," Annals of Disaster Risk Sciences, vol. 3, no. 1, Nov. 2020.

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[18] Mazzù A., Foti F., Tesfai Ogbu I., et al, (2019) D1.2 PANACEA User Requirements, PANACEA project, European Commission panacearesearch.eu/deliverables/d12-panacea-user-requirements

[19] E. G. Spanakis, et. al, "Emerging and Established Trends to Support Secure Health Information Exchange," Frontiers in Digital Health, vol. 3, p. 29, 2021, doi: 10.3389/fdgth.2021.636082.

[20] Chiarugi, F., et.al. Real-time cardiac monitoring over a regional health network: Preliminary results from initial field testing. CiC 2002 29, 347(50).