Henrique Martins'
Digital Healthcare
Systems

National Health Cybersecurity

Policies and Strategies in a Global Context

Policy paper

7th August 2020 - Henrique Martins

Abstract

This paper aims to explore the specificities of information security and cybersecurity risks in the health sector, pointing out to the need for specific policies, strategies and governance, both at national and international levels. It details health cybersecurity context and what are the peculiar risks and challenges in securing health cyberspace. It uses the Portuguese example to illustrate national level most relevant issues, the policies, strategy and governance adopted and how it established existing international collaboration mechanisms. It explores why and how individualized National Health Cybersecurity Policies and Strategies (NHCPS) make sense and could benefit from being conceived and deployed. Lastly, it analyses existing international cooperation in the area of health cybersecurity and advances alternative suggestions within the scope of existing inter-governmental organizations, including the eventual role of UN, WHO, or even NATO in this, increasingly important field of national and international defence – the health cyberspace.

1. Introduction

In most countries in the world, population is growing old (OECD, 2018), which, associated to unhealthy lifestyles, increases healthcare needs, leading to healthcare systems sustainability challenges (*Health at a Glance 2019*, 2019). Health 4.0 (Bause et al., 2019) means a possibility for organizational change through the implementation of new digitalization strategies and advanced information technologies. These, however, come with a new ever-increasing risk of "damage" to information. Cyber-attacks that impact or are directed to health units are ever more frequent due to the critical and intrinsic value of the information about humans which they harbour. There are multiple examples, often hitting public opinion and trust as they are mediatized. The Ransomware WannaCry, in 2017, which led to British National Health Service disruption of service with over 20.000 appointments cancelled and estimated costs of 90M£. Recently, a cyberattack hit the second-biggest hospital in Czech Republic amid the Coronavirus outbreak[1]. The attack to SingHealth (Commitee of Inquiry, 2019) where over 1.5 million patient personal data and medical records of over 160.000 appointments, including the prime minister's data, was exfiltrated in Singapore, a country known for its advanced cybersecurity policy, strategy and practices (Singapore, 2016). These illustrate that healthcare can suffer in large cyberattack events even in countries with renowned national cross-sectorial cybersecurity capabilities and strategy, as it poses specific challenges. This can justify a special attention is needed within national defence strategies.

Information availability, confidentiality and integrity are critical and depend on how good we protect information technology (IT). Defending information systems that manage our Operational Technologies (OT) such as lifts, electric power, water or heating is also needed. Lastly, there are information elements that depend on the human brain. We have our "information systems" inside, our Human Technology (HT), and these too, can be tampered by psychological, neuronal, or hybrid threats. Interest in "human factor" increases persistently and it is known to be the single most important factor in cybersecurity resilience. Although many such concepts exist for paper or non-digital based information, and relevant concepts and threats exist in that context, this work focuses on cybersecurity, in the sense of securing electronic and digital systems and their information. For this work, the European Commission concept of cybersecurity as a "*Set of concerns and actions taken to protect cyberspace, both in the civil and military domains, against threats resulting from the interdependency of its information infrastructures and networks*" (European Comission, 2013) seems useful. It helps us as it places cybersecurity realm into that of policy, leadership, managerial and even, academic, "concerns" and not just "actions". Sharing concerns about the topic is already a way to foster cyber resilience.

"Digital Health" is a priority worldwide, reiterated by the World Health Organization (WHO) (WHO, 2020). Admittedly, this may temporarily be conditioned by COVID-19 pandemics response, but it will come back to central stage. Digitalization of healthcare is expected to increase quality of care and clinical safety. Safety that is ever more univocally dependent on information systems security. A higher use of these technologies brings more efficiency and effectiveness to health and care, but the increasing dependency of productive processes on digital platforms raises risk surface and risk exposure. As healthcare digitalization progresses, tampered information systems will lead to increasing problems in health and care services and with higher potential, and real, impacts on individual human health. It is, therefore, paramount to break this negative cycle, thus enabling healthcare professionals and patients to take full advantage of the digitalization of the heath industry. This explains why there is more declared interest of governments and health organizations on cybersecurity. There is, however, a severe

[1] Media news about these attacks are available at: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/, https://hotforsecurity.bitdefender.com/blog/mysterious-cyberattack-cripples-czech-hospital-amid-covid-19-outbreak-22566.html; https://www.cybersecurity-insiders.com/details-of-covidlock-ransomware-and-czech-hospital-infection/

lack of strategizing, implementation of concrete actions and broad awareness to the severity of the matter. This work aims to help address this need, it's relevance and outlining and exemplifying elements of a country's **National Health Cybersecurity Policy and Strategy (NHCPS),** in a global context of **international cooperation**.

2. Healthcare Cybersecurity context

A global analysis from the *Protected Health Information Data Breach Report* (Verizon, 2019), points out "healthcare is the only industry in which internal actors are the biggest threat to an organization; assets most often affected in breaches are databases and paper documents, basic security measures are still not being implemented" depict a very low cybersecurity maturity in this sector. Based on European Network Information Security Agency (ENISA) studies (ENISA, 2017), until the approval of the NIS Directive, health was not seen as providing essential services, so less of a priority. Healthcare organizations are easy targets for malicious attackers, as lack of security awareness in involved stakeholders is high. Medical equipment in use (i.e. CAT scanners or MRI machines) can be outdated, and patch management complex. The natural vulnerability of medical devices adds to often unsecure wireless networks.

The *Global Digital Health Partnership*[2] has identified major challenges in health cybersecurity through its workstream on cybersecurity. These do not differ significantly from those at EU level, except the absence of overarching regulations and technical sharing forums in non-EU spaces. Due to the complexity of the health sector, the extent of the challenges is a result of numerous actors involved in respective processes (public health systems, outpatient and inpatient care providers, medical device manufacturers, pharmaceutical industry, etc.) and the variable degrees of cybersecurity maturity across the different actor categories.

2.1 Digital healthcare systems – Cybersecurity, interoperability and integrated care

There is a need to move quickly to Digital Healthcare Systems in all countries. Cybersecurity concerns should not stop this, but rather increase its urgency. Developing and deploying eHealth services that fit and optimize existing healthcare systems is crucial to improve their performance, access, comfort and efficiency. In order to fully realise the degree of protection needed over health cyberspace we need to quickly understand relevant health context. Besides, obviously requiring perhaps some of the highest levels of IT, OT and HT security, as digital healthcare systems become a reality, we will see an increase in the usage of multiple devices. These will be network-connected and many human-connected. The term IoT set to designate the *Internet-of-Things*, is particularly useful in the health context as progressively ventilators,

[2] The Global Digital Health Partnership (GDHP) is an informal collaboration of governments and territories, government agencies and the World Health Organization was created to support the effective implementation of digital health services. See more at www.gdhp.org

pacemakers, perfusion pumps and other medical equipment are ever more interconnected to each other, to the corporate information system, and to the human body and mind. It is now commonly agreed that all these technologies bring high benefits to citizens and health professionals in healthcare quality, sustainability and equity of access. They bring dependency on secure digital platforms, therefore preventing and mitigating damage to health cyberspace, as part of that value proposition. One of the biggest health organization challenges is to protect adequately patient data inside them but also, and increasingly, in inter-organizational transfer processes. This challenge brings together three interconnected topics which are very important for an effective, efficient, safe, sustainable and high-quality healthcare:

a) Healthcare cannot continue to be provided in stove pipes and isolated levels of care but rather in an integrated holistic manner;
b) For a) to be enabled by coherent patient data, information systems have to be interoperable, allowing data exchange between all types of health institutions and the citizen's home;
c) For b) to be realised without service disruption, data modification, exfiltration or loss, the highest possible levels of cybersecurity most be in place. This, however, without limiting what was outlined in a) and without making interoperability described in b) a technical and economically unsustainable effort.

As interoperability and interconnections increase at a global scale, additional threats to data integrity will result from networks of health information between organizations and countries with different maturity levels, different attack surfaces and distinct technical and political vulnerabilities. Adequate security strategies, which include a solid data sharing policy and inherent information exchange requirement, and a cybersecurity architecture, are needed for heath organizations to be able to ensure confidential data is properly protected while shared when needed. Citizens, not just as a patient or healthcare user, but as a source of digital data, permanently connected to the health systems, in different but progressively more intruding ways, are another aspect about health cyberspace which is becoming very important. Citizens are data sources when:

a) "Monitor" devices which are temporarily connected to individuals;
b) Home-devices capture direct (i.e., telemonitoring) or indirect data about us;
c) Wearing devices or "w*earables", like* smartphones or smartwatches;
d) "*Implantables*" (or implanted devices) are carried inside the human body. Implants like prothesis or pacemakers may have sensors and actants which run vulnerable firmware or software.

The distinction between c) and d) is very important for cybersecurity. The fact that in the case of d), unplugging the device from the person is not done easily and the technology is connected to a network which may have been compromised[3].

[3] In 2019, MiniMed® insulin pumps were redrawn from the market because of cybersecurity potential risk – Information available from the Food and Drug Administration (2019) "Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks:" *FDA Safety Communication* July 2019 available at: https://www.fda.gov/medical-devices/safety-communications/certain-medtronic-minimed-insulin-pumps-have-potential-cybersecurity-risks-fda-safety-communication

2.2 Normative cybersecurity context and international recommendations

Normative action on cybersecurity is recent in law, somehow older in soft-law, and there are some good old standing examples in selected industries by trade association recommendations, or industry standards. ISO standards and certification have played an important role, but they are not mandatory. Healthcare cybersecurity scenario is generally less developed than in industries such as aviation, electricity, or banking, as digital maturity in healthcare is relatively lower. In EU soft law, ENISA 's work is very relevant with multiple initiatives in health cybersecurity. The European Commission, mostly thorough its Directorate General for Communications (DG CONNECT), supports different research and collaboration initiatives. These led to joint efforts at national, regional or even local levels between different countries and between health and IT industries. They can indirectly influence policy and law making at EU and Member states level.

In US the watershed moment in information security for health was the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[4] leading health institutions and vendors to profound change, not just in privacy but in information security as it connects to privacy. The Directive (EU) 2016/11481 shortly known as the NIS Directive, is the first European legal document specifically targeting the improvement of cybersecurity throughout the EU. It includes health as an essential service, and it sets up a Cooperation Group. Member states must create a legal framework and identify Operators of Essential Services (OES) in their territory and comply with several binding provisions defined nationally and ensure to take appropriate cybersecurity measures. The directive recognizes healthcare providers (HCPs) – hospitals and private clinics – as OES. Criteria for their identification was not clear. As national laws transpose the directive, different interpretations, levels of ambition and different law-makers sensitivity to implementation capacity in the ground, have led to a very different sets of rules, resulting in a completely heterogenous landscape of OES in health. In a more connected EU health sector such uneven landscape increases cybersecurity costs, lowers predictability and reduces synergies.

The 2016 General Data Protection Regulation (GDPR, 2016) implies a new set of rules, with stronger enforcement on health data classified as a special category of personal data (art. 9º) specially obligations in case of data security breaches. The Cybersecurity Act (*Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification*, 2019) reinforced the role of ENISA, which has been tasked to prepare the 'European cybersecurity certification schemes' that serve as the basis for certification of products, processes and services. In particular, the Act establishes EU wide

[4] HIPAA law, or Public Law 104-191 was published in 1996 in the US, and subsequent regulation on privacy and security have been produced. Legal text is accessible at https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996, the website of the U.S Department of Health and Human Services has a vast list of resources about cybersecurity in health accessible at: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

rules and European schemes for cybersecurity certification of such ICT products, processes and services. This can, and will, influence healthcare domain in its use of indirect and even direct products and services, especially relevant regarding Electronic Health Records and Medical Devices. Regarding the first, the 2019 EC communication on the Electronic Health Record Exchange Format (EHRxF) plays a central role as it includes cybersecurity specifications as components in defining health exchange formats/profiles (European Comission, 2019b). Regarding the second, it is fundamental to look at regulation (EU) 2017/745 – Medical Device Regulation and regulation (EU) 2017/746 – In Vitro Medical Device Regulation (*REGULATION (EU) 2017/745* , 2017; *REGULATION (EU) 2017/746* , 2017). This regulation covers the information technology security provisions, including hardware and software, for all medical devices that all manufacturers of currently approved medical devices must follow and established also the Medical Device Coordination Group (MDCG). In late 2019, the MDCG released recent guidance on Cybersecurity for medical devices which can be useful harmonization and soft law mechanisms.

3. Portugal's National Health Cybersecurity Policy and Strategy (NHCPS)

Portugal has a publicly funded National Health Service (SNS) and operates as a hybrid heath system with parts of healthcare provision covered by non-public sector entities. The Ministry of Health (MoH) governs and defines national health policy, including setting up sectorial rules in Cybersecurity. The Serviços Partilhados do Ministério da Saúde (SPMS) is the organization providing shared services to health institutions in the areas of information systems, public procurement, telehealth, billing private sector organizations amongst other services, operating as a Digital Health Agency[5].It was appointed as the eHealth authority for cross-border digital services as well as for cybersecurity by sectorial legislation.

3.1 National eHealth and cybersecurity strategic level

Portugal's first National Strategy for Cyberspace Security had not reference to health. In 2019, the second version was approved (Governo de Portugal, 2019). Health is now fully included and the SPMS president is made member of the Superior Council for Cyberspace Security. SPMS, in alignment with MoH, is responsible for developing, implementing and monitoring the National Strategy for the Health Information Ecosystem (ENESIS 2020). The first one was adopted in September 2016, for the triennium 2017-2019 (Governo de Portugal, 2016, 2017b). SPMS reports[6] that initial work was carried out in order to ensure the alignment of the

[5] SPMS mission is to share knowledge, to cooperate and to develop activities for providing services in the areas of information systems, and promote the use of standards, methodologies and requirements that guarantee interoperability, interconnection and security of data. To see more details, check organizational website at www.spms.min-saude.pt.

[6] Draft cybersecurity strategy was made available in February 2020 for public consultation at SPMS website where a brief revision of previous efforts is included.

information security and cybersecurity national objectives to those of health organizations and ensure their alignment and capacity building. In 2017 two Ministry of Health Order were published (Order 1348/2017 (Governo de Portugal, 2017c) and Order nº 8877/2017 (Governo de Portugal, 2017a) as well as many compulsory instructions around and following the WannaCry crisis were emitted by SPMS to public sector but influenced non-public sector organizations. Such high proactivity and concern is in line with the level of maturity in digital health in Portugal which has improved substantially over the last few years, leading WHO's Europe to conclude, "*Portugal is now in the forefront of eHealth in Europe. The new NHS portal is a potential game changer for access to services information*" in its 2018 "Review of the Portuguese health system" (WHO Euro, 2018, p. 24).

The new strategy, ENESIS 2022[7], is more ambitious and aims to include the private and third sector, it is organized to address societal health challenges in it vertical domains, as well as sustain more horizontal structuring efforts, such as capacity building, tele-health, law and ethics and, cybersecurity. Cybersecurity in Health corresponds to a set of processes, people and technologies that ensure the provision of healthcare supported in information systems in a resilient and secure manner. The cybersecurity action plan was launched for consultation in February 2020.

3.2 Sectorial, national and local governance structures

There is no effective cybersecurity policy and strategy implementation without a clear governance architecture. Regarding governance at the sectorial level, Order nº 8877/2017, defines the set of rules that all entities of the National Health Service and the Ministry of Health (MOH) have to follow, the role of SPMS and which structures to create locally (Governo de Portugal, 2017a). In the context of cybersecurity incidents, health entities are required, according to Ministerial Order 1348/2017 to designate the Responsible for Mandatory Notification (RNO) of cybersecurity incidents that ensures the operationalization of the Centralized Mandatory Notification Procedure for Cybersecurity Incidents (NOCICS) of the entities of the National Health Service and the Ministry of Health to the CNCS and performs functions as the entity's single point of contact with the Security Operational Coordination Element (ECOS) of Health.

At national level, SPMS has been assuming a participative and collaborative role in cyber and information security among health-related organizations having the responsibility to define sectorial cybersecurity measures and procedures, established by the governance model for the implementation of health cybersecurity policy in Order 8877/2017. This also lists of specific

[7] The new strategy "ENESIS 2022" has not yet been published, but its public consultation version is available at the SPMS website in Serviços Partilhados do Ministério da Saúde (2019) Estratégia Nacional para o Ecossistema de Informação da Saúde - ENESIS 20|22 - Documento para consulta pública - https://www.spms.min-saude.pt/2019/10/consulta-publica-i-estrategia-nacional-para-o-ecossistema-de-informacao-de-saude/

and quite powerful actions including ordering and carrying out cybersecurity audits. In all public sector institution, structures and roles are expected to exist, namely, a Compulsory Notification Responsible; a dedicated Chief Information Security Officers (CISO) is recommended, and an Information security and risk committee (CRSI) is desirable.

If on the public sector side governance is clear, centralized and very detailed, the same cannot be said for the non-public sector healthcare providers. Here there is no obligatory structures and roles, except those that result from National level cross-sectorial law or guidance from the National Cyber Security Center. To mitigate this, two informal, voluntary processes were set in motion:

1) The celebration of voluntary cyber-security collaboration protocols, which can be signed by private institutions or associations with SPMS, establishing that these will follow similar rules and procedures, and benefit from same information sharing and collaborative environment.

2) The creation of the "*Grupo de Acompanhamento para a CiberSegurança*" (GACS). This group, where public and non-public health stakeholders were invited to participate in a progressive development approach, acts as an aggregation forum for concerns and experiences in health cybersecurity.

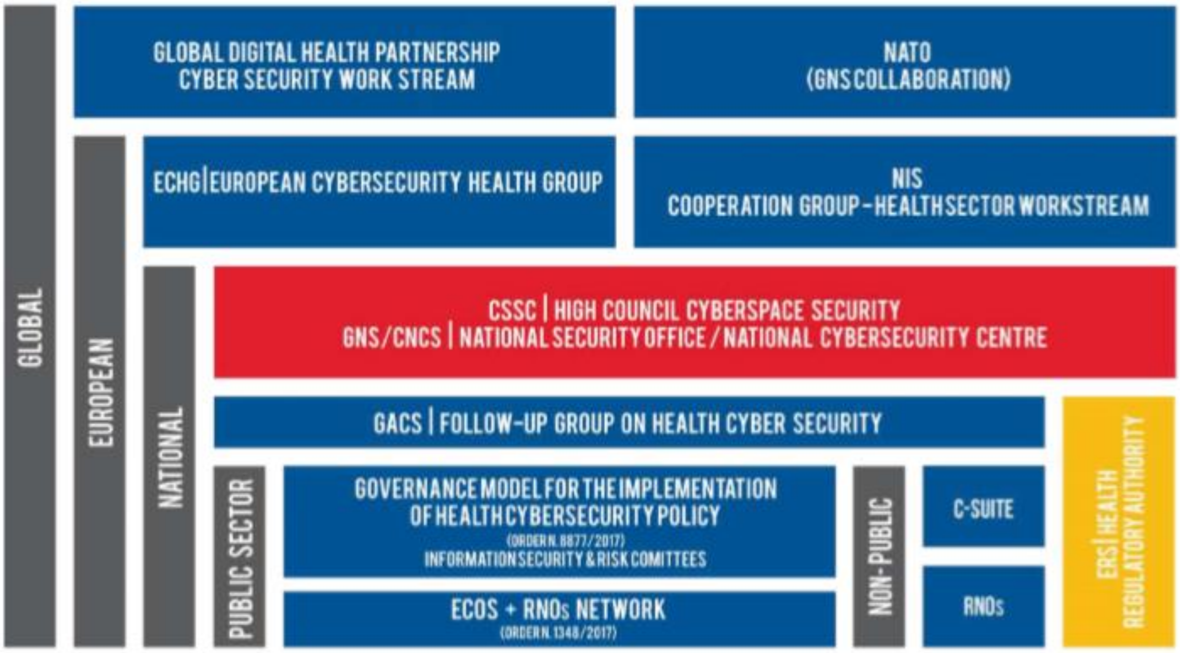
Cyber security dedicated structures at subnational level are very relevant and decisive. Ready and prepared health organizations with organizational "cells" and functions dedicated to cybersecurity allow better localization and realization of idealized plans and defined actions. Such plans and actions can come vertically from government directions or from shared and mutually agreed initiatives within voluntary cooperation spaces. Many countries have ISACs or CERTs for health, but often the focus of discussions on those fora are rather technical, and or dedicated to alert and response. The GACS was created with over 26 health entities, public, private and social administration bodies, associations, professional bodies, cybersecurity agencies, acting as a voluntary cooperation space at national level and a multidisciplinary consultative body for SPMS. GACS is also a policy thinking group and an operations experience exchange facilitator, in three domains: i) Prevention, Education and Awareness; ii) Response to threats; iii) Research, development and innovation. In the event of large "health focused" threats, risks and incidents that can affect all entities this group can facilitate better trans-sectorial articulation.

3.3 Supra-national health cybersecurity collaboration structures

Portugal shares a common legal and policy cybersecurity framework with other EU countries. Its policies are influenced by its participation in North Atlantic Treaty Organization (NATO), where aspects of cyber-defence are covered at the highest levels, and via both law enforcement and secret services international collaborations in the cyber-crime dimensions. No formal health cybersecurity policy influence existed until October 2019. For countries outside the EU, cybersecurity policy influences may come from NATO, while others may also participate in Interpol, but for the most part they are more isolated from a regulation and influence point of view, as organizations such as United Nations (UN), WHO or the Organisation for Economic Co-operation and Development (OECD) have no agenda in cybersecurity in health.

Portugal has made a significant effort to cooperate and develop international health specific cooperation in cybersecurity. Three forums where this is taking place are worthy of note. SPMS launched an European Health Cybersecurity Group together with 16 other Member States, the European Commission and ENISA in October 2019, the same month the new Commission Implementing Decision 2019/1765(European Comission, 2019a), included cybersecurity as a formal topic for policy work at the eHealth Network – the highest policy body for eHealth in the EU, created under the Directive 2011/24/EU . As a sequence the group was formalized in November 2019 at the 16th meeting of this *Network.* At European level, following the publication of the Network Information Security Directive (*DIRECTIVE (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union*, 2016), a cooperation group was created and on January 2020, under proposal of Portugal a *Workstream* dedicated to health was approved. Finally, at a global scale, it is worth mentioning the relevance of the informal collaboration under the (GDHP) where a workstream on cybersecurity was launched in Feb 2018. Portugal hosted the first two workshops and was chosen to lead this workstream as of December 2019 with the co-chairmenship of Hong Kong. These structures are in several states of maturity, very informal, which raises sustainability concerns and limits the breadth and depth of their work.

Picture 1 – Diagram representation of cybersecurity dedicated structures, from local (public and non-public) to global dimension which relate to health cybersecurity in Portugal. “C-Suite” – top management.


GLOBAL
EUROPEAN
NATIONAL
GLOBAL DIGITAL HEALTH PARTNERSHIP
CYBER SECURITY WORK STREAM
NATO
(GNS COLLABORATION)
ECHG | EUROPEAN CYBERSECURITY HEALTH GROUP
NIS
COOPERATION GROUP - HEALTH SECTOR WORKSTREAM
CSSC | HIGH COUNCIL CYBERSPACE SECURITY
GNS/CNCS | NATIONAL SECURITY OFFICE / NATIONAL CYBERSECURITY CENTRE
GACS | FOLLOW-UP GROUP ON HEALTH CYBER SECURITY
PUBLIC SECTOR
GOVERNANCE MODEL FOR THE IMPLEMENTATION
OF HEALTH CYBERSECURITY POLICY
(ORDER N. 8877/2017)
INFORMATION SECURITY & RISK COMITTEES
ECOS + RNOs NETWORK
(ORDER N. 1348/2017)
NON-PUBLIC
C-SUITE
RNOs
ERS | HEALTH
REGULATORY AUTHORITY

4. The need for National Health Cybersecurity Policies and Strategies

Healthcare faces many challenges when trying to secure its own information. Perhaps the most interesting is the unprecedented wave of new digital services, expectations, diagnostics and therapeutics, while for the most part, it runs on XX century processes and organizational mindsets, in a painfully long transition from paper base to digital-base care.

Healthcare need to have strong cybersecurity capabilities, and it could be argued that such should be ensured by following a national cross-sectorial approach. While some argue that National Community Emergency Response Teams (CERT)s and other structures can be enough, a national CERT, regardless of its power and scope, can only do what the information and IS "owners" allow them to do, more or less empowered by laws, not rarely loose as very often they are a result of complex negotiations between numerous stakeholders. Increasingly, however, trans-sectorial fora are accepting the idea that dedicated working groups in health make sense. Sectorial particularities, the growing proportion of health sector in modern aging economy's, and the nature of the business – to secure health, restore wellness and save human lives – means we are talking about the most "*precious crown jewels*" of all societies. This context justifies the instantiation in the health sector of the national and supranational principles, priorities and perspectives of cybersecurity enhancement through dedicated policies and strategy.

Individualized National Health Cybersecurity Policy and Strategy (NHCPS) make sense and can benefit from being conceived in such generic terms that can be applicable to an array of different healthcare systems and contexts, both within and outside the EU. This is because it is the best way to ensure "accountability and pro-activity" of the sector in ensuring it defends itself from cyberthreats. It is essential to engage Health policy makers, administrators and managers, and health professionals in adherence and compliance to a "national cybersecurity policy and strategy", but specially to "co-create" within those frameworks, their own "health version". This, alongside a set of governance and interconnected structures dedicated to focusing and cooperating about cybersecurity, ensures "ownership". As such policies and strategies are though and conceived, analysis that will follow, based on increasing evidence from real world and pass crisis, will show that without securing IT, OT and HT in health, there can pose even higher risks to citizens life and health.

National policies in health cybersecurity will be influenced by technological imperatives and state-of-the-art requirements well outside the influence of healthcare stakeholders. This does not, however, mean that "how" many of these are to be implemented, how intensively and how fast, is not subject to planning. These definitions form part of a health cybersecurity strategy, and can be influenced by the maturity level, perception of the impacts and their significance as well as available human and capital resources.

Health cybersecurity policies benefit from being co-created within national cybersecurity strategic frameworks, in close collaboration with national and international cross-sectorial agencies, incorporating EU and other regulation depending on the jurisdictions, and assuring state-of-the-art advice is listen to. They still should be authored by Ministries of Health and Care, as appropriation of knowledge and policy priorities will be higher. Such ensures the context of healthcare is more present, commitment is higher, and innovation in initiatives will be more enticed. The risk, however, is that lack of resources and multiple focuses of health institutions lead to low ambition or to a too slow rhythm of implementation of concrete actions. This can be offset with cooperation and benchmarking with other similar efforts in other countries, as comparing at home, with other sectors, may not be authoritative or even realistic.

A final reason behind the tremendous value in healthcare people creating their own national health cybersecurity strategy is that they will explore multiple questions such as: i) do we have an eHealth strategy? technical and human capacity? What financing opportunities can we use to upgrade our IT? iii) When we hire new staff and receive interns or students, what are their awareness and capacity in cybersecurity? iv) or, how can health collaborate with education sector, and professional associations to upscale the future workforce?

5. Key aspects for a National Health Cybersecurity Policy and Strategy?

Successful National Health Cybersecurity Policy and Strategy (NHCPS) depend on the capacity to galvanize other policy and strategy in eHealth and Digital Health, while at the same time intercepting National Cybersecurity regulation and orientations. Each country will have its national strategy for securing cyberspace, but as discussed earlier in this text, healthcare is increasingly more cross-border, international, and uses ever more digital internationally made available technologies.

Four enables of a cybersecurity strategy in health can be identified as well as four pillars that should not be neglected. The pillars are elements that should not be forgotten, although others may be identified in each context. They are essential insofar as overall strategy is very likely to fail if they are missing. These are:

1) ***Whole-of-government approach*** to health cybersecurity strategy
2) One ***strong agency responsible for digital health***, and within it, a cybersecurity specialized unit
3) A large, ***multi-stakeholder group***, capable of involving, encouraging and mobilizing all parts of the health system around cybersecurity efforts
4) ***International cooperation*** and outlook culture

These four pillars are, arguably, also fundamental aspects for a broader eHealth or Digital Health Strategy in a country. However, regarding cybersecurity exploring how and why these are important pillars is relevant. A whole-of-government approach to Digital health is needed, as it is not possible to progress to sophisticated levels of maturity without significant cross-sectoral work. The costs would be higher as well as the sense of fragmentation to the citizen. Regarding cybersecurity for health digital services it would be ridiculously expensive to maintain a highly mature CERT, or a SOC (Security Operations Center) exclusively dedicates to health without sharing some of its tasks, namely alert and information gathering with, with a cross-sectorial entity. On the other hand, healthcare users are "all" citizens in a country and professionals equally have other digital services to which they access for personal reasons even though in a healthcare working environment. This is due to the nature of the work, requiring long hours in dedicated facilities, like for example, intensive care units, or other shift-based work. Connecting to outside and interacting digitally is no longer possible to be fully segregated for these personnel. As such, health benefits from using generic frameworks, and even exploring lessons from defence ministry or banking sector regulator. Link to common approaches to higher education are also key. Healthcare is a human intensive sector, dependent on high-skilled professionals with long demanding training career were cybersecurity topics inclusion will prepare them to "day-one". Also risks while these professionals are still training as intern students or residents need to be mitigated.

The argument for the benefits of a single national digital health agency, its profile and its possible roles are a long topic, worthy of another paper, and without its controversies. On the other hand, having a single cybersecurity unit for the health sector is less controversial and clearly an element that any national strategy needs to clarify. One can see four scenarios, regarding the existence of a unit dedicates to health, with a mandate to orchestrate, audit and dictate cybersecurity efforts in all sector, together with a SOC capacity:

1) It does not exist
2) It exists, within a Nacional Cybersecurity Centre, which is cross-sectorial by nature;
3) It exists in a health institution nor solemnly dedicated to digital health
4) It exists inside a digital health competence Centre (with Digital health Authority)

In coherence with all previous text the first scenario is unacceptable. The second is possible, it may even be highly effective in the response to incidents and restoration of digital services, but it will fail to work significantly close to the sector for awareness, preparation, and mitigation of risks, and it would have to have the same approach for all the remaining sectors.. The third scenario falls in the debate of whether a country should have a Digital Health institution. I believe so. The fourth scenario is better than the third because if a cybersecurity unit is operating under the umbrella and leadership of an organization that is focussed on digital matters, it will have the capacity to worried with "other organizations" security enhancement, but also exert an important influence inhouse, thus securing critical national level services. This unit, however, should take care of cybersecurity as well as all the other aspects of information security. Not doing so, would make the approach potentially incoherent as many paper information sources still exist and will need to be preserved in the future, eventually having been digitalized and lawfully destroyed.

It also means more practical and less normative positioning, which closes gaps to other organizations before and, specially, during a crisis. Lastly, an important distinction should be made about Digital Health Competence Centres, and Digital Health Authorities. The later not only must be competence centres on the various relevant matters in Digital Health, but also, have invested authority by Ministries and Government at large. Such authority is key in incident response, but also in preparation as priority conflict at healthcare institutions tends to favour non-IT matters over issues with doctors, direct patient care, medicines or disease-related emergencies.

The creation of a large group with multiple stakeholders, is an ***essential feature*** of a successful policy and strategy for health cybersecurity, as it works as a consultation and cooperation forum for cybersecurity eHealth related policies, procedures and techniques. It should be capable of involving, encouraging and mobilizing all parts of the health system around cybersecurity efforts this makes it useful. MoH and their agencies need to accept they do not have all the technical knowledge and in health sector. Industry players, such as pharma or private providers, for example, are often part of multinational organizations so they can bring different knowledge and ideas on board, from their “mother” organization. This increases complexity but can prove useful for copying and hybridization.

International cooperation in health cybersecurity is not an add-on to the functioning of a national dedicated unit, or just a good opportunity for occasional exchanges. It is a pillar of defence in health cyberspace.

The four NHCPS enablers are: interoperability, conformance assessment systems and audits, enterprise architecture, and digital identification. Lack of interoperability leads often to systems misuse, or misuse of information sharing channels to ensure necessary health information reaches those who need it. Any investment in the standards-based interoperable ecosystem is a security enhancing investment in health where the use of internationally recognized standards for information systems, and electronic health records, has traditionally lagged.

Without a proper conformance assessment system, many of the definitions, not just on interoperability but also specifically on security requirements will not really be checked and verified. National level authorities will believe systems have a certain performance, as they dictate, determine, even legislate, but somehow through some process this needs to be checked for conformance. Not to rarely, definitions, recommendations and even legal obligations are decided, without previous conformance verification and audit after systems are in use, the authority is lost. This is a problem, not just in cybersecurity but with other dimensions of a properly developed and matured digital health ecosystem. The “normative-reality” gap is a big problem in cybersecurity because if a crisis happens, decision-makers tend to think based on the norms they have emitted. Actions are then suggested, based on those system attributes and capacity, soon to realise that response to attack fails, when “in theory” it should have worked. Conformance and audits, regular as well as unexpected can help close this gap.

A solid health system enterprise architecture and related information system architecture is the only way to know, at any given time, what systems relate to each other and, more importantly which systems support each organization’s core and non-core activities. These links are essential to understand the relative risk if a given information system in the ecosystem is compromised. Not just data breaches, but also, system performance issues, connectivity performances or system availability can put a given healthcare function at risk: ePrescription, eDispensation, hospital laboratory results, or lists of patients to be operated the next morning, to name a few examples. The May 2017 WannaCry incident showed these dependencies in the worst possible way: as they unfolded. An EA-based healthcare system would have the information granularity to simulate such consequences not just on the information systems, but, more importantly, on the business/provider layer.

The last of the four enablers is digital identification. Without a strong digital authentication, authorization and signature, information systems and OT may be very well technically protected but still unauthorized humans can have access to them. Since more cyber incidents seem to result from direct human action or negligence, this means securing systems access only to the right people, for the right set of roles, and in the right moments is key to information security. The development of national-wide solutions of this sort, is not just key to cyber resilience but triggers other benefits as process and technologies to support up-to-date patient, professionals and organization indexes must be created and sustained. Professional roles, the core and non-core system professionals must access for performing under those roles, and hierarchy authorization trees need to be defined and that is structural change in any healthcare system.

6. What could international cooperation look like?

In present times, international cooperation is paramount for successful NHCPS creation and implementation. The challenge is to see where and how such cooperation between Governments, National Agencies, and broad-base healthcare stakeholders could happen and what could the priorities. This means establishing an international agenda on health cybersecurity. Countries can collaborate informally, but formal collaboration under established international institutions is very important for reasons of sustainability and authority of produced guidelines, recommendation and warnings.

There are challenges in securing health cyber space in a context of complex technologies, that can be literally inside the human body, in a sector that deals with human lives, frail citizens and highly sensitive personal data. There are four trends that help understand why such efforts benefit from international perspectives:

1) Broader international standards adoption, and active digitization agendas. For example, the EC Communication on digital transformation of health and care (European Comission, 2018) and the recommendation on the EHRxF where a reference to common cybersecurity standards adoption is present;
2) Increasingly global market for medical devices (i.e. ventilators or implantable solutions), means that threats are less country than device or company specific;
3) “Digital patients” harbouring inside them or wearing on them different IT-enabled devices that support or even maintain their life, who move around the world;
4) Increasingly global healthcare workforce moving between countries as well as cross-border tele-health means health services and professionals, use and mobilize increasing amounts of health data, or provide care through information systems.

While a more interdependent world inhibits to sharing of risks and vulnerabilities as its not obvious who is attacking who anymore, on the other hand medical devices and software industries have never been so global and digital. The opportunity exists for sharing threat alerts, as well as experiences in awareness campaigns, processes and people-related cybersecurity issues. Such level and topics do not expose unwillingness to discuss risks, failure points, or vulnerabilities and focusses everyone in raising general cyber resilience even against internal and intra-organizational threats. Health cybersecurity collaboration, in its infancy at present and limited in the span of countries and the maturity of the debate, can be made more sustainable, more engaging and shared across stakeholder and, equally important, more spread between different countries.

6.1 International cooperation in health cybersecurity – current landscape

In Europe, the role of the UE and its institutions is determinant[8]. At the EU level the ECHG and the NIS Cooperation Group dedicated health workstream exist since October 2019 and the first semester of 2020, respectively. These are too recent forums. The European Medical Agency's (EMA) role is relevant regarding medical devices in the EU space, like FDA is for the US market, and other regulators in different jurisdictions. EMA does not maintain any sort of active collaboration space.

At a global scale, the UN[9] has gained higher interest in cybersecurity, and in 2017 it was particularly active, but it is not actively engaging its members on regular discussions and sharing. The World Health Organization has grown in its interest in telemedicine, eHealth and now Digital Health in general. Its recent Draft Global Strategy on Digital Health 2020-2024 (WHO, 2020), refers cybersecurity within the scope of broader concerns on health data (point 17.)[10]. While many would say that WHO should focus on core-health topics and public health issues, it should also be involved and eventually act as a platform for international health cybersecurity cooperation because it has experience in emergency response and authority over MoH, which often underprioritize this topic.

Finally, it is worth referring the role of the GDHP. In existence since February 2018, its Cybersecurity Work Stream is focused on strategies that can strengthen the processes and practices designed to protect healthcare devices, systems and networks as well as the data within them, from security risks and cyber-attacks.

[8] The European Commission, mostly through DG CONNECT, has worked on the topic of cybersecurity for quite some time. This DG funds a number or research and collaboration projects, in cybersecurity and more specifically on health-related issues in cybersecurity, there are currently 7 ongoing projects. As an example, the PROTEGO project (https://protego-project.eu/) is developing a toolkit and guidelines to help health care systems users address cybersecurity risks in this new environment.

[9] The UN work in cybersecurity was framed mostly around counter terrorism. More information at https://www.un.org/counterterrorism/cybersecurity

[10] It seems WHO has little experience in health cybersecurity policy, although recent events like the WHO cyber-attack in 2020 and the abundance of cybersecurity scams about COVID-19 which made WHO release its first communication on cybersecurity (https://www.who.int/about/communications/cyber-security), may increase this Organization's awareness for this topic

Many of the refereed cooperation forums are either too recent, from 2018 and 2019, too technical, or temporary in nature like EU-funded projects. Most countries outside the EU space seem to have lesser space for international cooperation in health cybersecurity, albeit many, like Eastern Partnership counties are in harmonization processes of their Digital Health strategies and could benefit from more intense sharing[11]. Many countries outside EU, can have varying degrees of maturity but all share similar threats and impacts. To defend this global health cyberspace, as it should be conceived, new possibilities for health cybersecurity international cooperation should be sought.

6.2 International cooperation in health cybersecurity – future possibilities

Current efforts should continue, eventually they can be expanded, and this is likely to be of benefit to healthcare systems and societies in the multiple countries in Europe and globally. This expansion can be thought in 3 dimensions:

1) Making existing cooperation in health cybersecurity more sustainable, structured and solid;

2) Expanding the stakeholders to involve including, amongst others: i) patient associations and professional scientific societies; ii) industry, from device and equipment manufacturers to software development companies; iii) research and higher education institutions, or iv) SDOs related to EHRs;

3) Happen with more countries and under the auspices larger more established international bodies, like NATO, OECD or WHO. In Europe, eventually using the Eastern Partnership (EaP) and/or Central European Initiative (CEI) to enlarge the debate and capacity building outside immediate EU influence. Likewise, in other regions organizations like the Association of Southeast Asian Nations (ASEAN), or the African Union (AU) should be more engaged with health international policies, and in the intersection with economical and wellbeing concerns ensuring the security of their increasingly digital national health systems.

Regarding the first dimension, in the EU space models of information sharing are needed to boost existing "willingness" and recently formalized collaborations. Following the example of maritime security[12], a digital common information sharing environment (CISE) can be created if an "*information sharing matrix"* has been mutually worked and agreed thereafter. This could involve EMA, ENISA, EC (relevant DGs), and Member States. At the global level, following this dimension means ensuring such collaboration could eventually be hosted, in a sustainable manner under the umbrella efforts of the UN regarding cybersecurity in general, or at WHO

[11] The EU4Digital initiative aims to extend the EU DSM to the Eastern Partner states. Through the initiative, the EU supports coordinated cyber security and the harmonisation of digital frameworks across society, in areas ranging from logistics to health. More information available at https://eufordigital.eu/

[12] In the maritime security area a common information sharing environments (CISE) was created (https://www.efca.europa.eu/en/content/common-information-sharing-environment-cise),

international. The first option could explore the recent United Nations Counterterrorism Center UNCCT which has cybersecurity in pillar 2 of it is program. On further analysis, initiatives on cybersecurity were significantly boosted after the UN resolution 2341 (2017)(United Nations Security Council, 2017a), These initiatives and the resolution, however, are not specific to health. As a matter of fact, in this resolution "health" appears one time in a preambular note about "*increasing cross-border critical infrastructure interdependencies between countries, such as those used for, inter alia, (...) and public health*" alongside banking, or water-supply. The UNCCT follows the #6th review of the UN Global Counter-Terrorism Strategy A/RES/72/284" where no mention of health is found(United Nations Security Council, 2017b). This brief analysis highlights that terrorist attacks to individual citizens via digital health tools is not envisioned as a real risk, because in this case itis not only about defending national critical infrastructures and networks and sharing experiences about it. It is equally about raising awareness in citizens about cyber risks, especially if their life depends on implantable or wearable life-supporting digitally enabled and connected devices which can be subject to personally targeted or untargeted terrorist operations. Likewise, it is about working with industry and government regulators about market access and post-market surveillance of digital health technologies. On the other hand, it means the UN initiatives could occasionally focus on health, regardless, but in synergy, with the role of WHO. WHO responsibility on cybersecurity of healthcare systems in undoubtful. It increases as it promotes their digitalization, and as it repeatedly promotes Digital Health as a path to Universal Health Coverage. You cannot have a role in promoting Digital Health adoption without structuring and or participating in a plan for defending it. While WHO is already collaborating with over 30 countries in the GDHP this is a very informal, recent, and non-authoritative forum. It could devise a collaboration plan to promote NHCPS development and a sustainable initiative to foster cross-countries and cross-stakeholders cooperation.

Regarding the second dimension, in much the same way each country benefits from a health sector multi-stakeholders' group to reflect, discuss and cross-stimulate work in cybersecurity, creating international consortiums of such nature, is not just possible but equally desirable. These should orbit an existing formal entity, and its rules of procedure need to balance and respect public and private interests. They can be assembled at a regional level, for example, around certain EU collaborations mentioned before or the proposed regional WHO cybersecurity groups. Likewise, large non-for-profit organizations such as Healthcare Information and Management Systems Society (HIMSS) or others digital health promoting consortiums, could create such multi-lateral international collaboration spaces provided they include national governmental people.

The third dimension points to the materialization of the two preceding ones. While globally the role of the UN and WHO, or of health sector led initiatives and large consortiums, there is a space for regional or inter-regional collaborations. For example, as extensions of the work in progress in the EU, organizations like OECD and CEI can cross-fertilize these efforts with small but relevant number of countries in more effective ways than global collaboration. Their tradition in health sector policy is already there, what is missing is to prioritize and find willingness of members to focus on Digital Health more intensely and in its securitization simultaneously. Although different in its shape and realm of action, but equally spanning EU and non-EU countries, NATO, with a longstanding cyber defence tradition, managed at the highest level, should play more attention to the health sector for three reasons:

a) health wearables and implantable devices are perfect vehicles of attack;
b) health organizations lag in cyber resilience, while the impact to their operations can put lives immediately at risk – healthcare is a double weak link;
c) non-health procedures and a culture of defence if introduced to health organizations could lead to leap-frog enhancements in sector's cybersecurity.

7. Conclusions and final notes

A wake-up call about healthcare security, and cybersecurity in particular, is still greatly needed.

From global to local we need to define policies, structure national governance, articulate international collaboration and professionalize health cybersecurity.

This issue is very specific yet worthy of attention by the highest levels of national and international policy. Health cybersecurity is an essential element of defence, not just of countries, but that of individuals, and their lives.

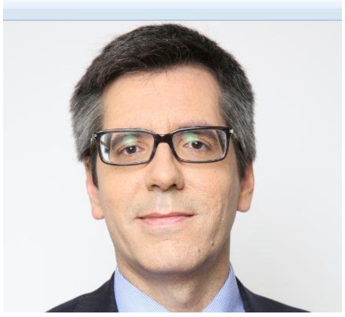
As we see a global discourse on increased speed in the digitalization of healthcare, and increased need for international collaboration, we need to make sure, Digital Health comes with solid defence. Otherwise, we think digital is good for health, but it may bring more risks than benefits.

Countries should implement National Health Cybersecurity Policies and Strategies (NHCPS) and be willing to support and contribute to international efforts and agencies where sharing of that implementation can help them and boost such needed efforts.

Inspired by WHO definition of health we could see information security and cybersecurity, as a total state of integrity, availability and privacy, and not just the absence of cyber-incidents. In a Digital Health environment cybersecurity concerns move from highly relevant to critical as the essence of the functioning of the health system depends on the "health" of the information systems that support it.

If you like to comment on this paper, or ask for more details or advise please email me at henrique@henriquemartins.eu and visit my website www.henriquemartins.eu

About the Author:



Henrique Martins, MD, PhD, FIAHSI. He has a Medical Degree, Internal Medicine Speciality, a Master and PhD degrees in Management, and is finishing his Master's in Law, studying Public Liability implications of AI in Health. He is a Medical Doctor and University Professor at a Medical School and two Business schools, teaching and researching in Digital Health, Leadership and Management education for Medical Students and Health Professionals. He is the past president of SPMS, Portugal's Digital Health Agency, where he led National eHealth efforts for close to 7 years, and the former Member States co-chair of the EU eHealth Network, the highest policy body on eHealth in the Union. He was elected Fellow of the International Academy of Health Sciences Informatics (within IMIA) in July 2020. He became National Defence Auditor, course 2018/2029 (IDN, National institute of Defense, Portugal) with final research project on health cybersecurity. He now works as an Academic in two high-ranked business schools and one medical school, as CMIO of Hospital Fernando Fonseca, Lisbon and on individual consulting projects in Healthcare Transformation and Digital Health.

8. Bibliography

Bause, M., Khayamian Esfahani, B., Forbes, H., & Schaefer, D. (2019). Design for Health 4.0: Exploration of a New Area. *Proceedings of the Design Society: International Conference on Engineering Design*, *1*(1), 887–896. https://doi.org/10.1017/dsi.2019.93

Commitee of Inquiry. (2019). *Public Report of the Committee of Inquiry Into the Cyber Attack on Singapore Health Services Private Limited'S Patient Database on or Around*. *January*. https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx

ENISA. (2017). *Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures* (Issue November). https://doi.org/10.2824/28801

European Comission. (2013). *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final*.

European Comission. (2018). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on enabling the digital transformation of health and care in the Digital Single Market; empowering citiz*.

European Comission. (2019a). *COMMISSION IMPLEMENTING DECISION 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019D1765

European Comission. (2019b). *COMMISSION RECOMMENDATION of 6.2.2019 on a European Electronic Health Record exchange format*. https://ec.europa.eu/digital-single-market/en/news/recommendation-european-electronic-health-record-exchange-format

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, (2016) (testimony of European Parliament). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR), REGULATION (EU) 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 Protec (2016).

REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical device, (2017) (testimony of European Parliament). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745

REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on, (2017) (testimony of European Parliament). https://eur-lex.europa.eu/eli/reg/2017/746/oj

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, (2019) (testimony of European Parliament). https://eur-lex.europa.eu/eli/reg/2019/881/oj

Governo de Portugal. (2016). *Resolução de Conselho de Ministros nº 62/2016*. https://data.dre.pt/eli/resolconsmin/62/2016/10/17/p/dre/pt/html

Governo de Portugal. (2017a). *Despacho 8877/2017*. https://dre.pt/pesquisa/-/search/108269312/details/normal?l=1

Governo de Portugal. (2017b). *Despacho n.º 3156/2017*. https://dre.pt/home/-/dre/106881538/details/4/maximized?serie=II&parte_filter=31&day=2017-04-13&date=2017-04-01&dreId=106872363

Governo de Portugal. (2017c). *Despacho nº 1348/2017*. https://dre.pt/home/-/dre/106415139/details/2/maximized?serie=II&dreId=106415113

Governo de Portugal. (2019). *Resolução Conselho de Ministros nº 92/2019 - Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. https://dre.pt/home/-/dre/122498962/details/maximized

Health at a Glance 2019. (2019). OECD. https://doi.org/10.1787/4dd50c09-en

OECD. (2018). *OECD Regions and Cities at a Glance 2018*. https://doi.org/10.1787/reg_cit_glance-2018-en

Singapore, C. S. A. of. (2016). *Singapore's Cybersecurity Strategy*. https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy/~/media/0ecd8f671af2447890ec046409a62bc7.ashx

United Nations Security Council. (2017a). Resolution 2375 (2017). *S/Res/2375*, *2341*(S/RES/2375), 1–9.

United Nations Security Council. (2017b). Resolution 77/284 (2017). *S/Res/77/284*. https://doi.org/10.5363/tits.7.8_44

Verizon. (2019). *Protected Health Information Data Breach Report*. https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pdf

WHO Euro. (2018). *Health System Review* (Issue April). http://www.euro.who.int/en/countries/portugal/publications/review-of-the-portuguese-health-system

World Health Organization. (2020). *Draft global strategy on digital health 2020 – 2024*.