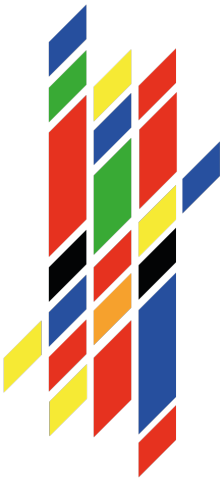

eHAction

Joint Action supporting the eHealth Network

Data and Systems Security Guide

Spring 2021

Grant Agreement nº 801558

Co-funded by the European Union's Health Programme (2014-2020)

Table of Contents

Acronyms

Acronym	Description
CEF	Connecting Europe Facility
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
CMMI	Capability Maturity Model Integration
CSIRT	Computer Security Incident Response Team
eHAction	eHAction – 3rd Joint Action supporting the eHealth Network
EU	European Union
GDPR	General Data Protection Regulation
EHR	Electronic Health Record
ENISA	European Union Agency for Cybersecurity
HCP	Healthcare Provider
ICT	Information and Communications Technology
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centre
NIS	Network and Information Systems
NCPeH	National Contact Point for eHealth
OES	Operator of Essential Services
PDCA	Plan-Do-Check-Act
WP	Work Package

Foreword

This Guide has been elaborated within the eHAction WP7 with the aim to provide an orientation and help navigate the different guidance documents that have been delivered by EU-level collaborative expert teams of Member State representatives and ENISA primarily under the 2016 Directive on security of network and information systems (the NIS Directive). A direct outcome of increased Member State co-operation in addressing the cybersecurity challenge in healthcare has been the publication of a growing volume of guidance, alongside the relevant standards, addressing governments and health and care providers.

Indeed, there is already a wealth of documentation on several aspects of cybersecurity providing evidence of the magnitude of the problem of cyberattacks and their consequences on healthcare organisations, information on how organisations have been tackling this problem, studies and proposals for action at national and EU levels and more recently specific and actionable guidance and resources supporting implementation of information security management systems by organisations.

The Guide assumes that national healthcare cybersecurity strategies and implementation frameworks are actively incorporating much of the knowledge produced at EU level. As such, they can provide the necessary direction to healthcare organisations in terms of common levels of protection to be achieved through the healthcare providers' projects. This is happening at different speeds and varies according to the organisation of national health systems. There is therefore a large potential for healthcare providers to leverage the European co-operation initiatives, including those undertaken under the NIS Directive, cross-border eHealth co-operation, and several collaborative projects supported by the EU in order to achieve their own cybersecurity objectives in the most efficient and evidence-based way.

Whilst the formal title of the Guide refers to the term '*data and systems security*', this term is taken to be equivalent to healthcare-contextualised use of the broader term '*network and information systems security*' used in the NIS Directive and the short term '*cybersecurity*' broadly used in the literature. These terms are used interchangeably in the document.

1. Why a Data and Systems Security Guide for Healthcare Organisations?

Information is the new currency of the modern world, one with ever-increasing value. Information security therefore gains importance and moves from a peripheral technical discipline to the core of any modern organisation, its concerns and processes.

The digital transformation of health and care holds significant potential for improved health outcomes, accelerated production of medical knowledge and increased health system intelligence. The stress and strain that the COVID-19 pandemic has exerted on healthcare organisations and health systems has exemplified the challenges healthcare is facing and has placed in context the integrated response that is necessary, including exploitation of high-performing data platforms, multivendor device connectivity, community-based care, remote monitoring, co-ordination of response and pooling of data for research and discovery of new drugs and vaccines. Connected medical devices, for example, can bring about increased patient safety and efficiency, particularly if connected to clinical information systems. When this applies to the whole healthcare organisation ecosystem, it becomes a 'Smart Hospital'. However, the increased flow of information within and between hospitals brings cybersecurity risks that 'Chief' level professionals in the hospital (CIO, CISO, etc.) need to address.

The risks include possible harm to patient safety or loss of personal health information and may not only be caused by malicious actions but also by human errors, system or third-party failures and natural phenomena. Healthcare is amongst the five most cyber-attacked industries over the past 5 years, along with manufacturing, financial services, government, and transportation[1]. Undeniably, there has been a considerable increase in cyberattacks in the healthcare sector, with significant material and reputational damage to the victims. These attacks can be driven by several motives: financial gain, theft of intellectual property, gaining of competitive advantage, or political motivation. Several reports of cyberattacks and risk assessments, both in the public and private sector, show that these attacks are not only more frequent but also more sophisticated and harmful.

As hospitals are increasingly becoming smarter and more integrated within healthcare ecosystems, they are also interconnected with ecosystems involving other sectors of the economy, such as other government sectors and financial services. This entails interconnecting numerous actors, critical assets, sensitive personal and financial information, resources and inevitably results in blurring boundaries between organisations and jurisdictions. Indicative of this interdependence is the fact that access to electronic medical records and health system data and to stolen medical data by an attacker might also be instrumental in opening bank accounts, procuring passports and even getting loans[2].

Hospitals still face the greatest risks, vulnerabilities and impacts in the case of cyber incidents. Broadly speaking, all healthcare organisations should understand and address the risks through well-defined and well-managed cybersecurity initiatives, delivering a holistic approach, combined into a single integrated framework and an overarching strategy involving the organisation's processes, people and technology, to ensure an effective defence. Over the

[1] Top 5 industries at Risk of Cyber attacks: https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#2fc5f5b5715e

[2] L. Coventry, and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," in Maturitas, 2018, 113:48-52

last decade, there has been an increased awareness concerning information security and cybersecurity. In Europe, the General Data Protection Regulation, the 'NIS Directive' (security of network and information systems) and the Cybersecurity Act[3], reinforcing the role of ENISA (the EU Agency for Cybersecurity) in orienting the Member States, are the clear political expressions of a new paradigm of encouraging organisations operating inside the EU to rethink their information and IT management practices. A direct outcome of increased Member State co-operation in addressing the cybersecurity challenge in healthcare has been the publication of a growing volume of guidance, alongside the relevant standards, addressing governments and health and care providers.

This Data and Systems Security Guide (the Guide) is intended to support healthcare providers in designing and implementing information security systems that are capable of protecting the healthcare providers' critical information infrastructure and information resources. This is pursued through supporting them to navigate the available guidance documents that are created collaboratively and maintained at international level. Such decisions are typically shared within the higher management executives in the hospitals responsible for procurement of equipment, ICT systems and related services. Thus, the Guide addresses Chief Executive Officers and Chief Information Security Officers. However, more management functions may be relevant in European hospitals and as such may also be addressed by this Guide.

[3] 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 https://eur-lex.europa.eu/eli/reg/2019/881/oj

2. Cybersecurity in Context of Healthcare Organisations

The cybersecurity challenge in healthcare organisations is two-fold: their environment is rapidly changing, becoming more connected internally, within the healthcare system and with other sectors, thus increasing the attack surface with a concomitant exponential increase of their security risk. Their potential for response is however hampered by outdated and complex legacy IT systems, that are vulnerable to cyberattacks and a lack of cybersecurity culture, competencies and technical capabilities.

Healthcare organisations are undoubtedly facing new challenges to provide and maintain reliable services in a fast-evolving technological environment. Today, most of the activities, processes and business are ICT supported and data driven; consequently, data and information have become highly critical assets in the organisation, requiring a high level of both privacy and security protection. Protecting these critical assets against security risks is further strained by the increase in connected systems and devices, and the need to exchange data outside the organisational boundaries, nationally and across borders. In fact, securing information and patient data is one of the biggest challenges the healthcare sector faces, inside and outside the organisation, when exchanging data electronically, between organisations (hospitals and other health units) or allowing access to data for research and other secondary uses.

Devices, system components and networks are becoming autonomous, ubiquitous and interconnected. As healthcare becomes more connected, the large volumes of data, stored and maintained in healthcare organisations, that are critical to patients and healthcare and financing systems, gets increasingly exposed to cybersecurity risks for the organisations and patients alike. Risk is further increased by the fact that, unlike credit card information, health data cannot be changed once stolen. As a result, health data are considered fifty times more valuable than financial information on the black market and therefore among the most targeted kind of data[4]. As a matter of fact, it has been noticed that data breaches are becoming more and more frequent in the healthcare sector. Threats to smart hospitals are not limited to malicious actions in terms of their root cause; human errors and system failures as well as third-party failures also play an important role.

Consequently, from a cybersecurity perspective, the definition of the challenge in healthcare organisations is two-fold: their environment is rapidly changing, becoming more connected internally, within the healthcare system and with other sectors; as the attack surface increases with the introduction of connected devices, the attack potential grows exponentially. Their potential for response is however hampered by outdated and complex legacy IT systems, nevertheless critical for the organisations, that are vulnerable to cyberattacks and failures, as well as a significant lack of awareness and training of professionals on cybersecurity issues and risks. These attacks, besides causing financial loss and reputational damage, diminish the trust of patients in the treatment and storage of their health information stored in digital infrastructure, which is a challenge for the organisation's digital innovation efforts.

[4] PROTEGO- Why addressing cyber risks in healthcare is needed https://protego-project.eu/2019/04/why-addressing-cyber-risks-in-healthcare-is-needed/

Information and data, within the healthcare context, are amongst the most valued assets, both for its legitimate and illegitimate use. Having access to the right information at the right time can help save lives, in a significant way, and increase the effectiveness of healthcare services and procedures, as well as reduce healthcare costs. When misused, it can cause serious harm, whether in the form of personal data theft, cyberattacks using ransomware and other modern ways to monetise on its malicious use or even worse: targeted attacks using falsified healthcare data, hijacking of medical devices and other similar techniques may be used to induce significant harm or even death.

A multifaceted response is therefore necessary starting from the adoption of strategies that can effectively tackle identified vulnerabilities, prepare and engage the workforce and inform their technology acquisition policies. People, processes and technology are the three pillars of more resilient and secure healthcare delivery and availability of health information with increased user confidence in digital technologies.

3. The Cost of Data and Systems Security

Organisations should analyse their needs and evaluate the costs and how much they can invest in downtime prevention. They should also plan for the cost of security measures, and understand and appreciate the costs of doing nothing, e.g. the financial impact of downtime and data loss.

It is well known that information security, if it is to be treated properly, is not a low-cost endeavour. From the management perspective, it often seems that the organisation's budget may be better spent on areas directly related to its core business, i.e. provision of healthcare. The cost of securing information was integrated in the ICT budget, and it was typically marginalised and overlooked. On the other hand, historically, most ICT systems were used to facilitate mainly administrative tasks, and direct threats and risks to patients were minimal.

As the digitisation of healthcare advances and healthcare becomes more connected, services become data-driven and with increased dependency on the availability and proper functioning of the ICT infrastructure. This significantly increases the cost of any malfunction, let alone of malicious action aimed at those devices and systems. Furthermore, the trend of wearables and home-used medical devices is on the rise, and thus the amount of information processed digitally and the reliance on ICT in the actual provision of healthcare services will further increase dramatically.

In the past, information security was mostly intangible, and it was quite hard to calculate the benefit gained or, at least, the cost savings of securing information in healthcare organisations. This task has become much easier, as one can simply calculate the cost of downtime of a crucial process such as a CT or MRI scan, as well as the cost of failure of the laboratory information system. Therefore, the cost of information security can be compared to the cost of its absence. There are direct impacts to the bottom line of the healthcare provider implied in any of those cybersecurity incidents, regardless of the root cause of the failure. And these are just the direct cost and losses of doing business.

There are reports of health organisations that, after suffering cyberattacks in the past years, such as ransomware and phishing attacks, have stopped regular operations after data was stolen, encrypted or deleted. A very well-known example of these cyberattacks is the so-called ransomware WannaCry which, on 12th May 2017, shut down hundreds of thousands of computers around the world, followed by messages from hackers demanding ransom payments, as a result of a phishing attack and lack of operating system upgrade. In the United Kingdom National Health Service, this attack caused disruption of several healthcare services, with approximately 20,000 appointments being cancelled, costing £20m over the course of a week and more than £70m in the subsequent clean-up and upgrades to IT systems[5].

Failure to provide sufficient information security may of course have very dire implications to the healthcare organisation. One must not forget that the penalties and lawsuits related to either personal data breaches or malpractice related to poor information security will increase dramatically in coming years and have to also be taken into account.

[5] The Telegraph October 11, 2018 https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/

To illustrate this, there are many variables that affect the cost of downtime, and they are not easily quantified. The cost of downtime depends on the type of organisation, the event that causes downtime, and indirect costs that will come from downtime; however, a simple exercise can demonstrate that the cost can be very high: How many doctors' appointments will be cancelled if we have an hour, a day, or a longer period of downtime? How many surgical procedures will be cancelled for a specific period of downtime? How many hours of labour will be lost?

For example, the unavailability of critical services will entail costs related to the impact on citizens' and patients' rights and freedoms. Making information unavailable due to information security flaws may ultimately serve as an argument that underlies the concept of data breach within the scope of the GDPR, which will consequently lead to costs related to investigations, costs of producing justifications and evidence to supervisory authorities, and may finally motivate the imposition of heavy fines under that European law.

There are also indirect costs, such as loss of reputation: if systems go down, organisations cannot meet their commitments. Re-doing work is another indirect cost, that is most of the time linked with loss of data which sometimes may not be recoverable.

4. Legal Obligations for Healthcare Providers

There are two broad areas of EU legislation and its transposition into national laws that define areas of legal responsibility for healthcare providers: the General Data Protection Regulation (GDPR)[6], for ensuring protection of personal data stored by them and exchanged with other organisations, and Directive (EU) 2016/1148 of the European Parliament and of the Council (the 'NIS Directive')[7], which recognises healthcare providers (HCPs) – hospitals and private clinics[8] – as Operators of Essential Services (OES), i.e. operators considered 'essential for the maintenance of critical societal and/or economic activities'.

The NIS Directive and the GDPR offer a chance to the health sector to build strategies to keep track of their data and systems, not only allowing compliance but most importantly managing their assets in an integrated way.

Cybersecurity and the GDPR

The GDPR provides the general framework, requirements and rules on health data collection and use which, in large part, apply uniformly to all Member States. However, despite its general application, the GDPR does allow Member States to adopt national-level rules on issues such as professional secrecy, use of data for scientific research, use of data of a deceased person and the processing of genetic, biometric and health data.

The GDPR requires that all processing of data has a legal basis and that appropriate safeguards are in place. The high financial and reputational cost of being in breach of the GDPR is a worry to hospitals. The lack of national or local guidance about the interpretation of how to comply with the GDPR for research adds to uncertainty in many countries today, which will hopefully lessen as countries update their national data protection laws. In contrast, the use of health data (for example, in EHRs) for direct patient care and internal quality monitoring is less of a problem to most hospitals. Cross-border care transfers are sometimes seen as a cause for concern, but if the transfer is within Europe and the purpose is to support safe continuity to a hospital patient receiving care whilst abroad, the legal basis should be the same as for a hospital's internal data use for direct care.

It is important to recognise that there are also legal bases that are applicable to scientific research conducted on personal data. These also cover special category data, under which most health data fall. Safeguards such as pseudonymisation can be used, provided that one remembers that pseudonymised data is still personal and has to be kept securely and only used for legally acceptable purposes (such as research). Although it is not always easy to anonymise clinical data whilst retaining its research usefulness; this method can render the data non-personal and not within scope of the GDPR. Good anonymisation practices can be applied to data before it is used for research.

Hospitals should therefore not see the GDPR as an obstruction to making better use of their health data, for learning and for research. However, they should take legal advice to ensure

[6] European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, https://eur-lex.europa.eu/eli/reg/2016/679/oj
[7] As defined in point (g) of Article 3 of Directive 2011/24/EU.

that they are adopting and complying with the right legal basis, and also take ICT security advice on how to safeguard the data being used for research.

As a first step, the healthcare organisation should seek expert legal advice to ensure that they are adopting and complying with the most appropriate legal basis for each and every situation of data sharing.

In addition, the healthcare organisation should appoint a Data Protection Officer who should be able to develop a suitable GDPR compliance strategy and see to its proper implementation and continuing compliance.

The organisation's healthcare workforce will need to develop new competences and skills and a critical understanding of the need to shift away from the currently prevailing culture of individual responsibility for data stewardship towards shared data use and shared responsibility. Likewise, it is important that legal professionals understand and appreciate the cultural and ethical peculiarities embedded in healthcare systems and provide effective support to decision making on soft law and accompanying measures and safeguards.

Healthcare Providers as Operators of Essential Services

The NIS Directive[9] concerning measures for a high common level of security of network and information systems across the Union, recognises healthcare providers (HCPs) – hospitals and private clinics – as Operators of Essential Services (OES), i.e. operators considered 'essential for the maintenance of critical societal and/or economic activities' and where 'an incident would have a significant disruptive effect on the provision of an essential service'. The Directive further formalises international co-operation and delegates responsibilities to the established Member State Co-operation Group and ENISA for delivering guidelines which are relevant and provide valuable support to OES.

In January 2020, the NIS Cooperation Group agreed on the proposal made by the eHealth Network, supported by DG SANTÉ and DG CONNECT, to create a work stream dedicated to healthcare (WS12), where the main goal is to exchange and promote best practices based on the experiences of Member States in addressing identification, mitigation and management of cyber risks in the health sector, especially when implementing the NIS Directive. Work Stream 12 is now operational and focuses on producing reference documents to assist all Member States in their efforts to implement the NIS Directive, aiming at a common sufficient security level of health-related digital and cyberspace technologies, and of their use, in the EU. Future updates of this Cybersecurity Guide will provide navigation support to documents published by the WS12 groups.

This Cybersecurity Guide provides navigation support to documents published by these groups.

While national governments have the responsibility to promote a culture of risk management, risk assessment and the implementation of appropriate security measures through appropriate regulatory requirements, responsibilities in ensuring the security of network and information systems as such lie, to a great extent, with operators of essential services and digital service providers.

[9] Directive (EU) 2016/114811 of the European Parliament and of the Council

The NIS Directive allocates responsibilities for:

- *Operators of essential services and digital service providers to ensure the security of the network and information systems regardless of whether they perform the maintenance of their network and information systems internally or outsource it.*
- *Healthcare organisations, as OES, to comply with security and notification requirements for operators of essential services; notification should be without undue delay, to the competent authority or the Computer Security Incident Response Teams (CSIRTs) of incidents having a significant impact on the continuity of the essential services they provide.*

National computer security incident response teams (CSIRTs) are a key component of the protection of the digital community from cyber threats. The NIS Directive establishes an EU Network of national CSIRTs for information exchange and mutual assistance and is expected to improve cybersecurity incident response; reduce resource impacts for implementing good security processes; and support the development of a unified international view of good cybersecurity practices for the health sector.

5. Implementation of Information Security Management Systems

Management Responsibility

Sustainable progress is linked to our ability to ensure information security and protection of data whether at rest, in use or on the move. At the same time, the dependence of the healthcare organisations' business processes on the proper deployment of secure digital platforms and their protection from subsequent exposure to cyberspace risks cannot be overemphasised.

Information security is a strategic choice and starts with unequivocal support of senior management. Support includes making resources and budget available for network and information systems security, together with commitment of senior management to information security as an imperative for the organisation, inspiration and nourishment of a cybersecurity and information security culture that starts with each individual and extends over all operational areas in the organisation. All staff must be aware of the cybersecurity risks and their role and responsibilities in containing them. The human resource department also plays an important role in the dissemination of the new culture for the existing and the new members of the organisation.

Critical processes in an organisation that provides health and care must duly consider cybersecurity as a key design element and ensure it is aligned with the organisation's governance strategic management and business continuity planning. In pursuit of this alignment, top management and CISOs should design appropriate measures that include identification and prevention of risks; protection; detection and reaction but also training and awareness raising; access control; functional segregation and organisation; and governance and elaboration of a set of metrics to assess their effectiveness in practice.

In order to introduce a sustainable information security management system in any healthcare organisation, it is advisable to introduce certain roles in the organisational structure or enhance current roles with new responsibilities and authority. It is crucial that responsibility for information security starts at CEO level, not least because of its significant impact on any organisation's operations and reputation. Information security is also an enabler, particularly in the digital transformation of healthcare. The possibility of introducing further automation and cost-effective processes (anything from surgical robots to remote patient care, patient workflows and administration of medicine) needs assurances regarding patient safety and, as a consequence, a high level of information and systems security.

Furthermore, it is advisable to introduce roles for an 'Information Security Architect', who is responsible for oversight over the design of all technologies, systems and processes related to information security, and an 'Information Security Manager', with respective responsibilities in terms of operations. These two roles should have the authority to examine every aspect of the organisation and its information systems and processes, and introduce measures aimed at increasing the overall information security.

As a starting point, it is recommended that top management of healthcare organisations

- *Appoints a Chief Information Security Officer (CISO) and a cybersecurity team with an appropriate skill mix to cover all critical areas of operation who should be able to develop a suitable Cybersecurity Strategy and co-ordinate the development and implementation of an Information Security Management System*

- *Introduces, amongst the team, roles for an Information Security Architect and an Information Security Manager*
- *Encourages cooperation of clinical, legal and security professionals; it is through their collective skills, cocreation and alignment that the most effective, efficient and broadly acceptable strategies and measures may be developed.*

Implementation

Information security is a complex topic and, in structured environments such as healthcare organisations, it may take considerable time to develop and implement. Challenges related to implementing information security are not only technical; they also involve changes in processes and the behaviour of all participating parties, including staff, vendors and even patients. With this in mind,

> *it is recommended to look at information security and its implementation in terms of a continuous effort and adopt a maturity model enabling assessment of the current level of achievement in various areas related to information security and the planning of future advancement, development priorities and goals.*

General ICT methods such as Capability Maturity Model Integration (CMMI)[10] can be introduced, as well as specific models developed for electronic healthcare, such as the Quintegra Maturity Model for Electronic Healthcare or Healthcare IT (HIT) Maturity Model developed by IDC Health Industry Insights[11].

Within the EU, the NIS Co-operation group and ENISA have been tasked with the elaboration of guidance and support of OES. ISO and its national counterparts have also dedicated a substantial amount of effort in producing information security standards. Most methods share a common basic approach based on a small number of key principles:

- *Know your assets: what data, devices, systems and processes related to your information and its processing are in place, what their value or importance is for the organisation and key stakeholders for the provisioning of healthcare, such as patients, staff, management, owners, authorities, etc.;*
- *Identify and manage risks: what harm can be done (or just happen) to your assets, what are the root causes, how probable it is, what you can do in terms of either preventing it from happening or minimising its impact;*
- *Implement, appropriately and proportionately to the risks posed, technical and organisational measures to manage the risks posed to the security of network and information systems and having regard to the state of the art;*

[10] https://cmmiinstitute.com/cmmi
[11] http://www.quintegrasolutions.com/eHMM%20White%20Paper.pdf
https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

- *Document and be consistent: implement a formal system to constantly monitor your assets and risks, increase awareness among all involved, improve your procedures and learn from mistakes.*

The risks that result from cybersecurity threats and corresponding vulnerabilities are typically mitigated by a combination of organisational and technical security measures taken by smart hospitals. Experience gained from analysis of attack scenarios has shown that vulnerabilities may be contained through a rigorous assessment and vulnerability assessment, adoption of effective enterprise governance for cybersecurity, and state-of-the-art security measures, monitoring and auditing, and careful consideration of security requirements when introducing digital innovation and IoT components in the hospital, as well as investment in network and information system components. Awareness and understanding of the causes as well as the impact and origin of the incident through reporting, assessments, research, investigation, and analysis, is vital to enable well-informed decisions.

In their effort to design and implement appropriate network and information security measures, healthcare providers may find valuable guidance in the CG Reference document on security measures for Operators of Essential Services[12], published in 2018, which provides a synthesis of common approaches to the security measures today in Member States and provides guidance on elaborating such measures, organised under four main cybersecurity domains, summarised in Table 1.

GOVERNANCE AND ECOSYSTEM	PROTECTION	DEFENCE	RESILIENCE
Information System Security Governance & Risk Management	IT Security Architecture	Detection	Continuity of operations
Ecosystem management	IT Security Administration	Computer Security Incident Management	Crisis management
	Identity and access management		
	IT Security Maintenance		
	Physical and environmental security		

Table 1. Domains of cybersecurity measures and security measures

Source: Reference document on security measures for Operators of Essential Services

The CG recommendations support implementation of NIS and its aim to 'significantly raise the level of security of OES in view of allowing them to face the serious risks posed to the security

[12] CG Publication 01/2018 - Reference document on security measures for Operators of Essential Services

of their critical information systems' with the aim of supporting their essential operations and ensuring the continuity of those operations.

Healthcare organisations may profit from the implementation of these recommendations, not only in terms of leveraging consolidated good and proven practices for ensuring a high level of security but also in terms of improving their compliance to the NIS related legal obligations.

In addition to this proposed framework used for the identification of suitable measures, the ENISA 'Procurement Guidelines for Cybersecurity in Hospitals[13]' provide a comprehensive taxonomy of healthcare threats and also lists the most common risks per type of asset subject to procurement in a hospital.

Healthcare threats taxonomy and risk identification provided in the ENISA procurement guide may be used as a starting point, for inspiration and as a check list when performing critical asset and risk identification.

A critical success factor in securing information in any organisation is the introduction of auditing procedures at all levels of the organisation of processes that relate to data and information processing and therefore to information security. It is also important to understand that auditing does not only mean conducting a formal audit of the overall information security management system once every year. It means that internal and external controls need to be established at many levels within the organisation and its various processes, structures and systems. What is even more important is that findings from these auditing procedures must be used for further improvement of the system. Only a fully functional Plan-Do-Check-Act (PDCA) cycle can provide a reasonable level of security over longer periods of time. As both the organisation and its external environment with its threats and risks are constantly evolving, being secure means being ready for all the threats that may come not only today or tomorrow, but also next week or next year.

Incident reporting in healthcare organisations, internally but also as part of their legal obligations, needs to be in a standardised form, enabling a comprehensive description and classification of the incident. The CG Cybersecurity Incident Taxonomy published in April 2018, although primarily elaborated to support the coordinated response to large-scale cybersecurity incidents, has a broader scope and covers cybersecurity incidents affecting the security of network and information systems in any sector of society. This incident classification does not exclude the use of additional taxonomies, such as healthcare specific taxonomies, should they be needed.

By maximising the incorporation of this taxonomy in the classification system you use to register incidents, your records will be shareable in the context of information sharing across borders, annual summary reporting under the NIS Directive, and international collaboration and information sharing.

While the CG guidance so far is intended to be sector agnostic, it can be easily profiled to healthcare environments. Nevertheless, health-specific guidance is expected to be delivered by the Health workstream of the CG and published in the NIS CG web page[14] which should therefore be regularly consulted.

[13] Procurement Guidelines for Cybersecurity in Hospitals
[14] https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

Complimentary to the CG guidance documents, ENISA has published a number of studies addressing in particular the health sector. Its 2015 study, entitled 'Security and Resilience in eHealth: Security Challenges and Risks'[15], investigates the approaches and measures Member States took to protect critical healthcare systems, having, as main goal, the improvement of healthcare and patient safety. It equally includes: the policy context in Europe and the legislation of the Member States; perceptions across Member States on critical assets in eHealth infrastructures; the most important security challenges and common security requirements; as well as relevant good practices that have been deployed in the Member States for eHealth security. Furthermore, it makes a set of recommendations targeting the Member States, operators of critical eHealth infrastructures, and the European Commission. The following are some of them, highlighted as having particular relevance to healthcare organisations:

Member States and healthcare organisations:

- should perform an impact/cost-benefit analysis of healthcare cybersecurity incidents and to use this as leverage for increasing investment in eHealth systems and infrastructure security;
- should set up information-sharing mechanisms to start exchanging knowledge and lessons learnt on cybersecurity issues, i.e. how to mitigate incidents, which are the security measures they take, etc.

A second study, published in November 2016, 'Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures'[16], looks in particular into challenges faced by smart hospitals and proposes key recommendations primarily for hospital executives:

Hospitals should:

- Establish effective enterprise governance for cybersecurity
- Implement state-of-the-art security measures
- Provide specific IT security requirements for Internet of Things (IoT) components in the hospital
- Invest in NIS security products
- Establish an information security sharing mechanism
- Conduct risk assessment and vulnerability assessment
- Perform penetration testing and auditing
- Support multi-stakeholder communication platforms (ISACs)

Further guidance on implementing Network and Information Management systems may be found in the ENISA 'Procurement Guidelines for Cybersecurity in Healthcare Organisations'.

[15] https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services
[16] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals/at_download/fullReport

6. Procurement for Cybersecurity

When procuring IT systems, medical devices and other products and services, it is important that cybersecurity considerations are duly considered, in view of the risks associated with each type of new product or service that will be introduced in the healthcare organisation.

On the supply side, manufacturers of information systems and devices used in hospitals are expected to comply with security requirements, build security into products from the outset, adopt secure coding practices and perform extensive testing. Security requirements should be clearly defined in the procurement phase and should be verifiable by means of certifications or proof of compliance to relevant standards. Many large organisations, for example, are adopting ISO 27001 and have certified their security management system.

It should also be kept in mind that attacks in healthcare organisations are not always direct. They often come through their supply chain, especially when suppliers are considered more vulnerable and have access to critical information and data. It is important to identify points of potential attacks in the supply chain and understand the severity of threats, their likelihood, and the ability of current defence mechanisms to detect and address them. Auditing the cybersecurity capability of the supplier to determine the degree of risks they pose to the organisation is also a proven good practice; audits to apply to both the supplier selection processes and ongoing performance monitoring processes. It is noted that the notification obligation to the healthcare organisations introduced by the NIS Directive may also require that it follows the supply chain. These provisions should also be foreseen during the procurement phase.

Procurement is therefore a critical function for cybersecurity. Conversely, the importance of cybersecurity in the hospital changes the way procurement professionals work and requires that they acquire relevant skills to collaborate with their IT departments at all stages of acquisition of IT systems, medical devices or third party services to identify the best ways to address the relevant challenges.

In February 2020, ENISA published the 'Procurement Guidelines for Cybersecurity in Hospitals – Good practices for the security of Healthcare services'. The report offers cybersecurity guidelines for hospitals when procuring services, products and infrastructure. It addresses primarily hospital procurement officers and CISOs/CIOs, providing the context for addressing cybersecurity in procurement. A threat taxonomy and a list of key risks associated with procurement are also presented. All this information is accompanied by quick guides providing insights as to how hospitals can use it in their procurement process.

7. Additional Resources

DG CONNECT is has a mission to enable a resilient and privacy-protecting digital single market in Europe through leadership and being the centre of excellence in network and information security and digital privacy policy, providing enabling legislation, co-/self-regulation, cooperation and other soft policy measures including the application and periodic review of the NIS and e-Privacy legislation. Its mission further includes ensuring a future of strong digital resilience and privacy protection by leading the research, innovation and deployment agenda for network and information security and digital privacy in the societal challenges and LEIT/ICT of Horizon 2020 and in the CEF, and focusing on innovative and next-generation systems and generic cybersecurity and privacy solutions. Within this context, it has been funding cybersecurity projects for the health and care sector, some of which are already delivering very relevant and valuable results. H2020 projects on cybersecurity and data protection are progressively making available online a wealth of useful deliverables[17].

The Commission's Directorate-General for Health and Food Safety (DG SANTÉ) has been supporting cybersecurity policies, especially through the eHDSI deployment projects which pursue a minimum level of security standards for eHealth competence centres. Cross-border eHealth deployment, currently pursued through CEF-supported national projects, is today realised within a common Audit Framework which includes an agreed minimum set of security measures for National Contact Points for eHealth (NCPeHs) and a formal process for external audit and approval to join the network of Member States exchanging cross-border health data. NCPeHs commonly store and manage sensitive health data: patient summaries and ePrescriptions; they are therefore also OESs and as such this framework may be seen as yet another relevant source of information. All in all, 31 information security readiness criteria[18] have been formulated, which NCPeHs need to address when deploying their services.

[17] For example, see https://sphinx-project.eu/, https://www.panacearesearch.eu/deliverables https://curex-project.eu/content/deliverables

[18] eHDSI Readiness Criteria check list https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/4.+eHDSI+AUDIT+SERVICES?preview=/37755327/75663732/eHDSI-ReadinessCriteriaChecklist_Wave2_v1.2.1_20190103.xlsx