Appendix 1[3]

Report of the

EXPERT PANEL ON EFFECTIVE WAYS OF INVESTING IN HEALTH

on

Access to health services in the European Union

[3] Although this report is entirely *fictional*, visuals and content have been drawn from original reports by the European Commission and ENISA.

EXPERT PANEL ON EFFECTIVE WAYS OF INVESTING IN HEALTH

Final opinion

(EXPH)

The EXPH approved this opinion at the 14th plenary meeting of **3 August 2020**.

About the Expert Panel on effective ways of investing in Health (EXPH)

The **Expert Panel on effective ways of investing in health** is an interdisciplinary and independent group established by the European Commission to provide non-binding independent advice on matters related to effective, accessible and resilient healthcare systems. The Expert Panel aims to support and inform national evidence-based operations and policymaking to improve the quality and sustainability of healthcare systems, as well as to foster EU level cooperation to improve information, expertise and the exchange of best practices.

The core element of the Expert Panel's mission is to provide the Commission with sound and independent advice in response to questions (mandates) submitted by the Commission on matters related to health care modernisation, responsiveness, and sustainability. The advice does not bind the Commission.

The areas of competence of the Expert Panel include, but are not limited to; primary care, hospital care, research and development, prevention and promotion, cross-border issues, digital service infrastructure, clinical information systems and patient registers, health inequalities, etc.

Abstract

Member States of the European Union (EU) have **a clear mandate to ensure equitable access to high-quality health services** for everyone. This means ensuring that relevant, appropriate, and cost-effective health services can be accessed by all EU citizens anywhere within the EU.

DigiSantEU was founded to execute this mandate. In 2015, EU Member States unanimously agreed to the establishment of **DigiSantEU**, an EU-wide healthcare digital database. It functions by mainstreaming digital service infrastructure across all Member State healthcare institutions to ensure easy and immediate access to up-to-date electronic patient health records, including medical history, treatment reporting, diagnostic data and imagery. These data and services are accessible by any healthcare provider – clinic, hospital, private practice - within the EU when required to give treatment to any EU citizen.

Between 2015 and 2020, Member States made significant progress in improving access to healthcare through DigiSantEU. The number of people reporting unmet healthcare needs due to cost, waiting time, equipment and appointment availability fell steadily from 26.5% in 2015 to 3.1% in 2020. The waiting times for access to urgent and emergency medical treatment for citizens travelling within the EU also fell significantly. This marks tremendous progress in ensuring the equitable access to healthcare for all.

However, this success should not allow for complacency. The establishment of an eHealth digital service infrastructure connected across the EU introduced a new set of security and resilience challenges, particularly with healthcare providers identified as *Operators of Essential Services* by the majority of Member States. Five years on, the digital security of healthcare services has never been more important as cyber threats become more complex and unpredictable. These threats continue to challenge the ability of Member States to ensure fair, equitable, reliable and secure access to healthcare services.

The Commission therefore mandated this Expert Panel to identify, via a series of interviews with subject matter experts including hospital managers, policy makers and regulators (ministries of health), medical device manufacturers and cyber security experts with a focus in healthcare, the core challenges presented in the healthcare sector in relation to digital service infrastructure security as well as to provide advice on how healthcare operators can improve resilience going forward.

This Report therefore addresses:

1. The mandate of ensuring equitable access to health services and the responsibilities of the EU and its Member States;
2. How this mandate is operational through DigiSantEU's digital service infrastructure;
3. The cyber security challenges posed, as identified through a series of interviews; and
4. Key good practices to be reinforced on the operational level (in particular in hospitals) to bolster Member States' digital service infrastructure security.

(1) Roles and responsibilities of the EU and Member States in ensuring the equitable access to healthcare for all

The EU Charter, EU Treaty and the International Covenant on Economic, Social and Cultural Rights all establish a universal right of access to core health services. Interpretation of these documents suggests there should be progressive realisation of the right to health, requiring countries to move forward and, by implication, not to adopt measures that are regressive. Core obligations constitute a universal floor, not a ceiling.

Since 2015, Member States have proven to accept responsibilities beyond this for their citizens, by adopting the Decision to create and join **DigiSantEU**, establishing a right of access to health services for every citizen across the EU. Assuring this right is the joint responsibility of Member States and the EU: **primary responsibility lies with Member States,** with the EU mandated to complement national policies towards improving public health, preventing physical and mental illness and diseases and removing sources of danger to physical and mental health.

The Commission's Communication on the Transformation of Digital Health and Care 2015 identified the digitalisation of health and care sectors as the best means to facilitate equitable access, and DigiSantEU was therefore established based on three core pillars:

Pillar 1: Secure data access and sharing
To facilitate greater access to cross-border healthcare, DigiSantEU provides an eHealth Digital Service Infrastructure to securely exchange electronic health records between healthcare providers. DigiSantEU provided the means to optimise digital service innovations, to streamline data management processes, harmonise security regulation compliance, and establish a standardised electronic health record (EHR)[4] format for secure access across borders.

Pillar 2: Connecting and sharing health data and tools for research, faster diagnosis and improved health
To tap into the huge potential of health data to support medical research with the aim of improving prevention, diagnosis, treatments, drugs and medical devices. Healthcare providers can also access the diagnostic network to use tools and facilities remotely, better harmonising the diagnostic capabilities of all providers across the EU.

Pillar 3: Strengthening citizen empowerment and individual care through digital services
Digital services can empower citizens, making it easier for them to take a greater role in the management of their own health, in which healthcare can be accessible wherever it is needed. This allows citizens to fully benefit from the EU digital single market and freedom of movement in accordance with the TFEU and the 2011 Directive on patients' rights in cross-border healthcare. This also addresses the rising demand for healthcare and allows for better integrated and equal healthcare systems.

(2) DigiSantEU's digital service infrastructure

Following the DigiSantEU 2015 Decision, an EU-level DigiSantEU Committee was established with a representative from each Member State to establish the procedures and processes required to make the DigiSantEU service operational. In December 2015, national healthcare institutions across the EU were able to install the required hardware and transfer and upload data from prior hardware/software models to DigiSantEU's relevant systems, as determined by the Committee. This transfer was supported by the Connecting Europe Facility (Broadband and Information and Communication Technologies) programme, following the pre-agreed guidelines of the eHealth network to ensure

[4] ENISA defines an electronic health record is a "repository of information regarding the health status of a subject of care, in computer processable form. An EHR provides the ability to share patient health information between authorized users of the EHR and the primary role of the EHR is supporting continuing, efficient and quality integrated health care".

appropriate governance, establishment and successful operation of the digital service infrastructure. New Member States are required to follow this same protocol when joining.

Centralised **clinical information systems (CIS**) are used to support the interconnectivity of DigiSantEU across the EU. CIS include any kind of software oriented towards medical care such as hospital information systems (HIS), laboratory information systems (LIS), radiology information systems (RIS) and picture archiving and communication systems (PACS). All CIS must be located within the medical building or in a data centre facility under complete control of the IT division of the medical centre.

In the case of retrieving patient information, the **radiology information system (RIS**) is a core electronic management software used to keep track of patients being treated and their progress. The RIS generally manages patient tracking, appointment requests and scheduling, results reporting and image tracking. The RIS networked software acts as a computerised database that is able to store, manipulate and distribute patient information and allows for real-time updates of patient treatment, accessible by any DigiSantEU establishment. Specialised RIS software ensures the speed of workflow when using the system.

Picture archiving and communication systems (PACS) are used for the storing, retrieving, presenting and sharing of medical images produced by medical hardware devices. The PACS server works closely with the RIS software and is used to store all diagnostic imaging files. PACS replaces hard-copy based means by more effectively handling the enormous digital files and images generated by medical devices, for example by x-ray and CAT scans. It allows for instant searches and access to patient medical images as well as off-site viewing and reporting, enabling practitioners in different physical locations to access the same information simultaneously.

The RIS-PACS software is highly integrated and allows hospital radiology departments and diagnostic centres to function more effectively as patient EHR's, including medical history and diagnostic data and imagery, can be securely stored, retrieved and transferred. The effective integration of all CIS systems is central to the functioning of the DigiSantEU system, and the success of effective delivery of patient care and workflow is dependent on the advancement and prosperity of these systems.

Medical devices and diagnostic tools are used to generate the medical results and imagery stored and include any piece of hardware dedicated to treatment, control or diagnosis such as: radiology equipment, radiotherapy, nuclear medicine, intensive care equipment, robots for surgery, electro-medical equipment, infusion pumps, spirometry devices, medical lasers, etc. It also includes any diagnostic tool, implantable device or wearables (Internet of Medical Things technology) that communicate by electronic means with the IT systems of the hospital.

Industrial control systems manage all physical aspects of hospitals such as power regulation systems, door lock systems, close circuit security systems, HVAC systems, alarm systems, water, heating, auxiliary power units, security access, elevators, fire extinguishing, etc. Nowadays, control of all these systems is managed through particular software systems: Building Management Systems. Whilst not a formally integrated part of the DigiSantEU digital service infrastructure, the functioning of DigiSantEU services is heavily dependent on the effective and robust control systems of each hospital connected.

Professional services also contribute to the service infrastructure of DigiSantEU, which include all kind of services, outsourced or not, provided by professionals or companies: medical services, transportation, accounting, engineering, IT, legal, maintenance, cleaning, catering, etc.

(3) Cyber security challenges in the healthcare sector

This study focuses on one part of the vast healthcare ecosystem: the hospital. The hospital is considered as a collection of assets (infrastructure, software, systems, devices etc.), and cyber security should be explicitly addressed in all its different components. Many systems, products or services used by hospitals introduce or are characterised by significant cyber security challenges. Hospitals should work jointly with IT, security or risk departments to identify the best ways to address the relevant challenges.

Information presented in this report is the result of information analysis following a series of interviews. The interviews were conducted with subject matter experts from hospitals, policy makers or regulators (ministries of health), medical device manufacturers and cyber security experts with a focus in healthcare. The report was validated by the experts participating, as well as the ENISA eHealth Security Experts Group.

According to the interview findings, the most challenging type of infrastructure was "Clinical Information Systems" followed by "Medical Devices" and "Industrial Control Systems." Based on feedback, several key challenges associated with the security of eHealth digital service infrastructure were identified, including those used for DigiSantEU. These challenges have been grouped based on the previously defined types of infrastructure.

Type of infrastructure	Vulnerability factor	Challenges and threats faced
Clinical information systems	Full continuous operation	The interconnected ecosystem of a hospital has to be resilient as the requirement for real-time data analysis is high. Healthcare organisations usually operate 24x7, and resources are scarce, therefore, stopping a modality or even a desktop computer can seriously impact service. If a component fails this can cause unavailability of a system, which can have cascading effects on other healthcare systems and severely impact processes that rely, e.g. on the real-time collection of patient data, such as glucose measuring devices.
	Infrastructure incapable of handling system/ poorly designed or programmed	There can be unexpected challenges when installing new systems. New systems may appear sluggishness due to factors such as; (i) under rated server CPU or small system memory, (ii) lack of disk space generating disk errors, or (iii) network bandwidth unable to handle data traffic. Systems can also be poorly designed or have a poorly programmed system which can lead to erroneous results, system errors due to lack of input validations or user errors due to poorly designed user interfaces. This may be a particular issue with legacy systems.
	Component vulnerability	Information systems in healthcare organisations are typically made of different components from different suppliers. The streamlining of systems through DigiSantEU has helped minimise the problem of a wide supply pool and therefore exposure to different component vulnerabilities. However, another threat persists in that a vulnerability of one component used by all could generate more far-reaching effects.
	Software failure	Any piece of software can have errors. Many software systems are dependent on other software platforms; if one platform experiences an error, this can result in cascading software failures. This a particular challenge due to there being only a few specialist healthcare software developers. Servers are more prone to failure, not only because of failures in the software design but because they also rely on other software platforms (operating systems, programming frameworks, databases) that can fail.
	Interoperability	Some interoperability challenges across healthcare systems remain where antiquated legacy equipment used prior to joining DigiSantEU is still operational. The use of undocumented web services, delays in system updates and attempts to retain outdated system configurations can generate exploitable vulnerabilities. This creates systemic risks to the connected EU-wide healthcare system. New discoveries in medicine and innovations in technology and medical tools have the potential to increase interoperability if hospitals introduce new systems and devices to deliver additional services outside the capabilities of all DigiSantEU providers.
	Malicious targeting of legacy systems	Lack of procedures in place to patch or update firmware is a top security threat for hospitals. In healthcare organisations, IT systems are strongly interconnected and difficult to isolate without generating service disruption, creating a comfortable ecosystem for malware. Legacy systems offer back doors to malicious actors. Ransomware is perhaps the most known threat for healthcare organisations, due to the Wannacry case in 2017, in which a ransomware spread exponentially, taking advantage of a vulnerability present in 5% of the UK National Healthcare System (NHS) computers, which were still running outdated and unsupported software. Healthcare infrastructure can be considered an easier target because of two factors; (i) software infrastructure is hard to keep updated because it's very difficult to get a downtime slot, (ii) there are devices that can only run on specific legacy software and cannot be updated, which can act as malware reservoirs.

Medical devices and diagnostic tools	Hardware design errors	Any piece of hardware can have design errors. Special security measures are taken for medical devices and diagnostic tools that could generate physical damage if an error occurred, such as infusion pumps, electrosurgical units, ventilators, medical use lasers, or radiology and radiotherapy equipment. These latent errors may arise under certain circumstances during the normal use of the device. Most of the time, these errors are known and cannot be mitigated because the device cannot be updated.
	Legacy devices	Medical equipment such as diagnostic tools are typically very expensive; these devices are expected to be in service for many years. Due to this long lifecycle, maintenance support from manufacturers can be difficult, particularly when they change hands or close. For this reason, vulnerabilities cannot always be corrected and can thus be exploited.
	Hidden functionalities	Medical devices and diagnostic tools are complex to manage and set up. The habitual action is to leave this equipment in a standard setup, including default passwords and active functionalities, which can generate infrastructure vulnerabilities. These vulnerabilities can be exploited by malicious actors, for example, through the hijacking of hardware, medical device tampering or the mechanical disruption of imaging devices such as MRI machines and CT scanners which can be remotely controlled. Medical equipment typically requires real-time communications, and clinicians need a quick response system for patient data or test information. Dedicating processor time or communication capacity to respond to functionality problems impacts performance and in turn, the provision of healthcare.
	Device and data theft	The cost of medical devices is very high; medical equipment theft is a very common crime. With most devices using factory default credentials and physical access frequently granted to non-authorized or poorly trained personnel, it allows for the potential manipulation, damage, theft or loss of equipment or information assets stored. The threat of cyber espionage also exists. Interest of multinational pharmaceutic industries or other interest groups on clinical research results or patient data can act as key drivers for this type of threat. Intellectual property theft is now commonplace, particularly when it concerns new technologies and tools.
Industrial control systems	IT/OT hybrid solutions	Hybrid solutions make possible the convergence between digital and physical worlds, ranging from smart buildings to digital twins, and include for example real-time location systems for patients and valuable assets, diagnostic tools, pharmacy systems, or surgery blocks. This opens a new scope of threats that must be prepared for.
	System failures	Operating systems that coordinate activities among computer hardware devices can have different causes of failure. The most common include software or firmware failure, device failure, network failure, insufficient maintenance, or overloading.
	Network and medical server failure	A network failure can have devastating effects. Most of the main hospital centres form a hub between the main building and its associated centres - mostly radiology or ambulatory or day-care centres. Redundancy designs are crucial when mitigating this type of threat. Failures in medical servers (which control access to the hardware, software and other resources on a network) can occur as latent errors and, in some occasions, can prevent the service from functioning. Frequent server failures deteriorate medical care and degrade confidence in the institution.
	Power supply	Loss of electricity can also be of importance depending on the equipment affected. Intensive care units, operative rooms, servers and clients are usually protected by uninterruptible power sources or batteries but other equipment such as MRI or CT machines can be compromised. This can happen via natural phenomena, human error, power supply failure etc.
	Supply chain failure	ICS based failures can also be caused by supply chain failures, e.g. by the cloud provider, network provider, power supply provider or by the manufacturer of medical devices, not putting adequate care in the supply chain integrity.
	Insecure network and	Due to the use of insecure network protocols (HTTP), attackers can enter an organisation's network. Open ports on a device can also be used as an attack vector or

	access protocols	through known service passwords of an administrator's login. Poor physical security of building management system controllers and workstations can also allow attackers to physically install malware or sabotage devices.
	Target of malicious actions	Unprotected communications between medical devices and servers can result in information tampering. Sophisticated man-in-the-middle (MITM) attacks can change the data coming from vital signs monitors, laboratory, pathology reports or even images coming from CT scans, MRI or ultrasound systems on their way to the PACS server. Denial of Service is a very common cyber operation that can render servers at a healthcare organisation inoperable, especially due to the reluctance to use public cloud infrastructure in which the capacity of servers can be limited. Ransomware is also a particularly harmful type of malware that is used to target control systems.
Professional services	Human factors	Threats caused by human errors can include medical system configuration errors (such as not changing factory-default passwords), absence of audit logs (allowing for the trace of breaches), unauthorised or lack of access control procedures as well as bring-your-own-device (BYOD) policies without appropriate security measures in place.
	Target of malicious actions	Compromised emails (e.g. through spam and spear-phishing) are the dominating attack vector for malware infections. Clinician email addresses are available through hospital public directories or online. Most organisations still allow access to private mail web accounts. Here, an employee can open a document or link attached to a convincing email that contains malware. Keeping an adequate user awareness is very difficult. Multiple factors have been blamed: most personnel in the health field have little technical knowledge, work in an intense and stressful environment, as well as factors such as shift work and staff rotation.
	Patient privacy and safety	The lack of involvement of IT security department in setting up and managing medical systems and equipment as well as lack of staff risk-awareness can generate information leaks that could impact on reputation, patient privacy, penalties, or even patient safety. In healthcare organisations there are two specific conditions that make information systems different from the rest; (i) Patient data is permanent and cannot be changed if privacy is broken (as you could do with your credit card number for example), and (ii) cyberattacks can become physical and cost human lives. Clinicians work hard to improve patient safety - medical devices and IT services must be considered another layer of this.

(4) Operational-level good practices

Whilst DigiSantEU is an EU-level initiative, responsibility remains with nation states and national healthcare sectors to ensure the security of its digital service infrastructure while maintaining cross-border interoperability. EU legislation on medical devices, cross-border healthcare, data protection, electronic identification and security of network and information systems (etc.) offer a range of opportunities to facilitate digital resilience in healthcare. Moreover, numerous standards, governmental regulations, best practice guidelines, and scientific papers discuss cyber security and provide recommendations.

It is imperative that nation states, healthcare providers as well as CIS and medical device manufacturers, at a time of increased reliance on information systems such as DigiSantEU, keep up to date with both national and EU-level regulatory frameworks and security requirements. In order for all stakeholders to fully benefit from and trust systems, services and tools, they must be properly designed, implemented in a cost-effective way and provide a proficient level of security and privacy. **The deployment of healthcare ICT systems is an entirely national competence**, in which this Panel has collected a series of key good practices, based on findings derived from the expert interviews and in association with the ENISA eHealth Security Experts Group, to mitigate risks and increase systematic resilience on the operational level.

Practice 1: Access management

Physical access to digital assets should be regulated and authenticated via suitable technical measures (e.g. badges). One important route for the delivery of malware and for data theft is via portable storage media such as universal serial bus (USB) memory sticks. Therefore, on the operational level, organisations should consider disabling USB ports to prevent malicious software delivery or lock down physical ports to only trusted connections.

This strongly ties to the importance of strong user authentication, as a baseline security element for ICT products in healthcare. Strong authentication mechanisms for all systems, devices and networks should be put in place, with access privileges fine-grained. Preferrable, administrator-level privileges should be limited as much as possible.

Practice 2: Cyber security awareness and training

It is best practice to ensure that internal staff and external contractors working on premise are adequately trained in the healthcare organisation's security practices and rules on a periodic basis. This should include awareness training on cyber security risks associated with digital service infrastructure, including threat signals for malware, hacking and phishing scams, as well as key digital hygiene themes such as password protection, user authentication processes and risks associated with BYOD.

Practice 3: Patch and update all components

It is crucial to ensure updates are implemented, including applying software patches and keeping anti-virus software up-to-date. Patching is a basic requirement and there is a procedure to be followed, as set out by the supplier of the relevant hardware or software. The supplier should also include the role of the hospital IT professionals in this process and present a redundancy plan in case the patch did not function as expected.

This should be incorporated into an *update policy* by the hospital. Processes within this should include to: create a registry IT asset inventory of all current hardware and software running including previously installed versions; regularly investigate if new patches are released; test the proposed patch in some machines before taking the decision to patch all machines; determine the most suitable timing to apply the patches; and document the update procedure. Software and hardware updates should not be scheduled simultaneously.

Practice 4: Implement a vulnerability identification and management process for all infrastructure

Ensure that vulnerabilities are considered and identified before installing new products or services and that vulnerabilities of existing products/services are monitored throughout their lifecycle. This includes having an established vulnerability management process to monitor and address vulnerabilities of digital service infrastructure. Information on existing vulnerabilities may be obtained from the manufacturer or from public sources, such as the NIST vulnerability database.

A study published by ENISA found that the two most critical system categories for cyber security as being interconnected clinical information systems and networked medical devices, therefore a clear management process must address adequate measures such as firewalls and network defences. A whitepaper by the National Electrical Manufacturers Association (NEMA) provides a list of resources that support healthcare institutions in establishing an effective IT security program and management process.

Practice 5: Plan network, hardware and licence requirements

It is important to plan network, hardware and licence requirements in advance and determine the digital topology (how new devices will be connected to the systems). Assess whether the new systems, services or devices require third party software or whether the system will use current software but requires additional licensing. Hardware requirements (disk space, bandwidth, CPU capacity, memory) must be assessed against current capacity usage, to determine whether additional upgrades must be made before installation to accommodate the new system.

Ensure that the IT inventory is appropriately updated when any component is added or removed from the ICT environment and that baseline security configurations for ICT components exist and are managed appropriately.

Practice 6: Segregate your network

Sometimes the inherent vulnerabilities of devices connected to the network cannot be mitigated: for example, legacy devices that cannot be upgraded to newer operating systems. To protect the existing IT infrastructure from these devices, compensating controls must be implemented. It is important to isolate all network connected devices from the rest of the network. With network segmentation network, traffic can be isolated and filtered to limit or prevent access between network zones.

Whenever a medical device must use an old version of operating system known to have vulnerabilities it should be maintained off the network. Instead, a PC gateway should be developed to communicate with this device to obtain the data and pass it to the network, implementing encryption.

Practice 7: Establish incident response and business continuity plans

After creating the network and components topology, an incident response plan should be developed in case of failure. It should be clear what the role of the hospital and supplier is in case of service interruption, including the cost of the supplier's services, the response time expected and what redundant systems will be used. Different disaster scenarios must be thought out when planning.

If failure of a newly acquired system may jeopardise the hospital's ability to provide core services, a business continuity plan must also establish the strategy (replace the device or change faulty components), the means and procedures necessary for an organization to keep its critical services available under the worst of circumstances. Periodic tests of incident response and business continuity plans should be conducted.

Practice 8: Regular backups

Regular backups are an important action that can resolve many incidents that could critically impact digitalised hospitals. Comprehensive backup strategies include securing backups in the cloud or physically storing backups offline, as well as confirming the organisation's ability to rebuild systems and restore data. Backups should be made frequently (i.e., at least daily, a continuous or real-time backup is ideal). If using a cloud provider, it should concretely state where the hospital data is stored. The hospital should demand that sensitive data remains in EU borders (so that EU data protection regulation applies). Providers should also explain which encryption mechanisms are being used and provide redundancy and business continuity plans in case of an incident.

Practice 9: Allow auditing and logging

Generated logs are a crucial part of the secure-test-analyse-improve strategy of security. If we assume that sooner or later a system will be compromised, logs are one of the most useful tools to trace back how incidents occurred. The extent of information compromised can also be evaluated. A secure Central Logging System should be created to keep a copy of the logs so these files can be safely off-site in a secure location.

It is highly recommended that all organisations develop a network and user activity monitoring system that conducts surveillance for suspicious activities such as receipt of email messages from known fraudulent sources, unexpected changes in key files, unknown processes encrypting files or significant increases in network traffic. The implementation of intrusion detection systems is highly recommended, which can effectively monitor networks or systems for malicious or suspect activity in real-time.

Practice 10: Encrypt personal data at rest and in transit

A policy for systems, services or devices processing General Data Protection Regulation 2016/679 (GDPR) Article 9 special categories of personal data must be defined and constantly enforced. In cyber security, three states of data are distinguished: "in use," "at rest," and "in transit." Whilst data cannot be fully encrypted while being used, health information data must always be encrypted when "at rest" or "in transit." Encryption is one of the most common solutions used in hospitals, mainly because of the criticality and sensitivity of the data. As used for DigiSantEU data transmissions across the EU, communication security is provided using state-of-the-art, standardized security protocols, such as TLS (Transport Layer Security) for encryption.

Practice 11: Notify and comply

Legislation plays a significant role in defining the cyber security requirements for hospital digital service infrastructure. The Network and Information Security Directive (NISD) 2016/1148/EU has two main goals: the implementation of minimum-security requirements and the establishment of cyber security notifications for both Operators of Essential Services and Digital Service Providers. Under NISD, operators of essential services must take appropriate security measures and notify serious cyber incidents to the relevant national authority. All medical devices, software systems and digital service providers operating within the national healthcare service must comply with the security and notification requirements under the Directive.

The Directive also ensures cooperation among all Member States, through a Cooperation Group, in order to facilitate the strategic exchange of information among Member States. The CSIRT Network promotes swift and effective operational cooperation on specific cyber security incidents and shares risk-based information.

The GDPR also treats health data as a "special category" of personal data which is considered to be sensitive by nature and imposes a higher standard of protection. Organizations processing health data have specific obligations to report

data breaches which are likely to result in a risk to the rights and freedoms of individuals within 72 hours of a potential breach. If a data breach incident impacts the continuity of health services, it must also be reported according to NISD.

Practice 12: Establish supplier eligibility criteria

Whilst mitigation measures can be implemented by system users, others must be considered part of the system design and can only be implemented by system developers. It is therefore imperative to establish security baseline requirements and translate them into eligibility criteria when selecting suppliers. The EU has facilitated this process for DigiSantEU digital service infrastructure suppliers. For example, the Medical Device Regulation (MDR) provides specific provisions related to IT security for all medical devices, with published guidance for manufacturers on how to fulfil essential requirements. The EU has taken a step further in regard to DigiSantEU - by approving specific manufacturers and models for digital service infrastructure compatible and approved for DigiSantEU system users, for both security and streamlining purposes. A shortlist of those who meet the necessary standards and regulations are distributed to Member State healthcare authorities.

Practice 13: Utilise EU-level bodies and resources

In accordance with Article 3 of the Cybersecurity Act 2019, ENISA is tasked with the purpose of achieving a high common level of cyber security in the healthcare sector across the Union. ENISA will provide advice, expertise and support to the sector as well as for other relevant Union stakeholders. It will work to set out updated legal measures, regulations and administrative provisions related to cyber security. Such tasks and aid given are developed through ENISA's own resources, including technical and human capabilities and skills.

There are several ways in which the EU can further facilitate Member States in their mandate to ensure the equitable access to healthcare for all, such as: approving new regulations on medical devices and systems; promoting effective coordination between national authorities in implementing the regulations; stimulating cooperation between Member States for the development of eHealth digital solutions and exchange of good practice; contributing to the development of information systems and assessment methods; and promoting R&D in medical devices, systems and optimal use strategies.

Conclusions

The review by the Expert Panel concluded that despite national compliance with EU-level regulations that support the mandate of ensuring equitable access to health services for all, as well as security regulatory requirements for national digital service infrastructure, more is needed to ensure cyber security on the operational level. Security of the healthcare sector is a national competence, with support available at the EU level, which should be optimised to ensure the security of the DigiSantEU system in particular. The publication of this Report hopes to reinforce, in light of the forecasted challenges presented by the Panel, that Member State healthcare operators should better utilise EU-level support to ensure digital service infrastructure security, which will in turn further unify security practices across all connected systems and strengthen DigiSantEU 's response to cyber security challenges going forward.