December 2023

HOPE Position on the EU Cybersecurity Framework

The evolving European Union (EU) legislative framework for cybersecurity is of paramount importance to hospitals and healthcare institutions in the context of increased data exchanges facilitated by an ever-growing array of connected, interoperable digital systems, devices and applications accessed across different locations.

Day-to-day hospital operations and healthcare provision relies increasingly on connected digital technologies, which must be forcefully protected from the disruptive, burdensome, immensely costly and potentially harmful effects of cyber-attacks. Given that international hacking networks are increasingly bold in their intentions and causing major damage, both economically and societally, the expansion of the EU cybersecurity framework reflects a mounting awareness that joining forces and expertise to tackle vulnerabilities in the digital realm is as important as ensuring an adequate military defence capacity.

Taking a holistic approach, this paper outlines HOPE perspective on the EU cybersecurity framework in light of the growing threat affecting hospitals and healthcare institutions, including its practical implications and potential gaps. All things considered, within the overall EU strategy, it is particularly important to develop comprehensive strategies in the sector, build up leadership and skills, ensure proper integration between cybersecurity and other digital policies (including health data sharing, data protection, privacy, fundamental rights), and to earmark sufficient and flexible resources. At the same time, it is important that cybersecurity measures match users' needs and competences, and that they fit into everyday workflows without compromising care provision.

By creating pan-European resilience structures and stipulating vital measures to be taken by critical entities, the EU cybersecurity framework aims to increase capacity to prevent, prepare for, detect, manage and recover from cyber-attacks.

Healthcare, a major target

Digitalisation in healthcare is ubiquitous, today ranging from interoperable hard-and software to AI-powered solutions and robots, Internet of Things-based connected components, sensors for remote monitoring, cloud computing, and digital imaging to the many medical devices, wearables, and mobile applications carried and operated directly by health workers, patients and others. In a number of Member States, telehealth has also become a part of routine care. Overall, though, the roll-out of digital health is still very uneven across the EU on account of marked differences in financial investments and other resources, attitudes towards data sharing, and levels of digital maturity. Nonetheless, the healthcare sector is particularly volatile as every digital asset – including smartphones and tablets – provides a potential entry point for cybercriminals.

Cyber-attacks in healthcare are often instigated with the intention to compromise the confidentiality, integrity and availability of patient and disease-specific data, at worst putting human lives at risk; they also generate severe monetary and social consequences due to privacy violations, disruption of care and business continuity. They can take many forms, involving data leaks, system blocking and file encryption; the triggers are often simple but well-disguised phishing e-mails containing malware. Conscious of the crucial function of data in healthcare institutions and laboratories, the objective of cyber criminals is to obtain fast payoff in return for unblocking the systems. Apart from upsetting day-to-day health service provision and negatively impacting on performance (examples being cancelled appointments and postponed treatments due to the inability to access patient EHRs and specialist equipment, transfer of patients to other hospitals for acute care and life-saving operations), such incidents also compromise health research and can result in long-term reputational loss of affected healthcare institutions.

Regrettably, cyber incidents increased dramatically during the COVID-19 pandemic, when capacities were already overwhelmed. In 2020, the European Union Agency for Cybersecurity (ENISA) reported a combined 47% increase across the EU compared to the previous year[1]: in France, the number of declared cases even doubled in 2021[2].

In May 2021, the Irish Health Service Executive (HSE) became the victim of a particularly vicious ransomware attack that temporarily paralysed many healthcare services. Ransomware is a type of software ("malware") that enables the encryption of important files, thereby making it impossible for their owners to access them. Triggered by a phishing e-mail that contained a malicious attachment, the attack enabled the perpetrators to illegally access and copy the personal, financial and medical data of around 90,000 individuals, some of which highly sensitive[3]. As a result of the attack, thousands of medical appointments had to be cancelled, resulting in delayed treatments and longer waiting lists, while hospital staff were forced to revert to working with paper records. The costs to the HSE were reported to be massive (over 80 million by December 2022) while the broader costs, whether related to the health impact on individuals or to potential litigation, still remain to be quantified.[4]

ENISA's threat landscape report for the health sector covering January 2021 – March 2023[5] confirms the increase of cyber incidents affecting health organisations. During the period analysed, health providers reported 53% of the total incidents (European hospitals alone accounting for 42%) whereas 47% of cases were notified by "other" institutions including health authorities, bodies and agencies (14%), the pharmaceutical industry (9%), health research entities (11%) and supply chain and service providers (11%). However, it is unclear how strongly the European health sector is affected compared to other vulnerable sectors such as banking and manufacturing.

[1] https://www.enisa.europa.eu/news/enisa-news/on-the-watch-for-incident-response-capabilities-in-the-health-sector

[2] https://esante.gouv.fr/sites/default/files/media_entity/documents/mss_ans_rapport_public_observatoire_signalements_issis_2021_vf.pdf

[3] https://www.gov.ie/en/news/ebbb8-cyber-attack-on-hse-systems/

[4] https://www.irishtimes.com/crime-law/2022/12/12/cost-of-hse-cyberattack-rises-to-80m-letter-shows/

[5] https://www.enisa.europa.eu/publications/health-threat-landscape

Importantly, ENISA highlights that ransomware was one of the principal threats (54%), both in the number of incidents and regarding its impact on health organisations. 43% of ransomware incidents were coupled with data breaches or data theft as well as service disruption. Patient data were the most targeted assets (30%).

This worrying trend reveals the growing awareness of cyber criminals that health data, which are often private and sensitive by nature, can be lucrative assets. Ransomware facilitates extortion due to the combined threats of public exposure and reputational loss. In addition, distributed denial of service attacks (DDos), which target systems and services make it impossible for users to access relevant data or other resources, also saw a rise during the reporting period, especially in early 2023 and linked to pro-Russian hacktivism.

Although in the EU, larger Western European countries were the main healthcare targets during ENISA's reporting period (France notified 43 incidents, Spain 25, Germany 23), the risk is global and criminals can easily shift their geographic focus; similar experiences have been reported across North America, Australia, Asia and South Africa. The perpetrators are frequently either international cybercrime networks (83% of crimes were undertaken for financial gain) or politically / socially motivated hacktivists (10% were linked to ideology, 1% to espionage). That being said, ENISA highlights that more incidents are being flagged every year as a result of policies encouraging reporting, whereas during the COVID-19 pandemic more human errors in handling data systems occurred, e.g. due to misconfigurations and poor security practices. Confirming findings of other incident reports[6], ENISA notes that unpatched vulnerabilities in healthcare (from operating systems to applications) represent an emerging trend, intensified by the increased use of connected medical devices.

Despite the growing number of attacks and the enduring acceptance of remote working, awareness of cyber threats differs profoundly between countries and many hospitals and healthcare institutions remain ill-prepared with few or no cybersecurity resources.

EU cybersecurity legislation: Key components

Considering the growing size and multifaceted character of the threat, HOPE thinks that the development of an effective EU cybersecurity policy framework is timely and indispensable. Several components have already been endorsed by Member States, others are currently under negotiation by the EU co-legislators.

The EU's policy action on cybersecurity picked up steam 2013 with the publication by the European Commission of the first EU Cybersecurity Strategy and a proposal for a first EU Cybersecurity law (the Directive on security of network and information systems, called NIS 1 and adopted in 2016), and with the inauguration of the Europol Cybercrime Centre. This was followed in 2016 by a Communication on Strengthening Europe's Cyber Resilience System and in 2017 by the publication by the European Commission of a Cybersecurity package (inter alia granting ENISA a permanent mandate and stipulating a European certification scheme) and a proposal for a Cybersecurity Act.

[6] https://ciras.enisa.europa.eu/

The *Cybersecurity Act*[7] entered into force in 2019. It grants a permanent mandate to ENISA and assigns it more resources and new tasks, such as setting up and maintaining voluntary European cybersecurity certification schemes, supporting operational cooperation at the EU level, and helping Member States to handle cybersecurity incidents upon request.

The most recent EU "Cybersecurity Strategy for the Digital Decade"[8] was released by the European Commission in 2020 as the centre piece of a second package. Its primary goal remains to shield key economic sectors from malevolent hackers and incidents while protecting EU values and fundamental rights. But whereas the 2013 Strategy's priorities merely laid the building blocks of EU level coordination in this area to assist the Member States, and measures contained in the updated 2017 version aimed at further boosting the EU's cyber resilience, the new Strategy offers a more strategic and comprehensive vision.

An important part of the EU digital strategy is the Recovery Plan for Europe and the Security Union Strategy 2020-2025. It is comprised of regulatory, investment and policy initiatives to boost resilience and technological sovereignty, increase operational capacity to prevent, deter and respond to threats, and foster global cooperation. It also provides a policy roof for the legislative initiatives described below. A number of other EU initiatives and projects were funded in parallel.[9]

The revised Directive on measures to ensure a high common level of cybersecurity in the Union (*NIS 2 Directive)*[10], also released in 2020, was adopted in November 2022, entered into force in January 2023 and has to be transposed by 17 October 2024. It enlarges to new sectors the scope of 'high criticality' (healthcare providers were already included under NIS 1). It raises data security standards and imposes cybersecurity risk management and reporting obligations to a wider group of medium-sized organisations. In health, this includes manufacturers (covering medical devices and in vitro medical devices, wearables, telehealth solutions, pharmaceutical products and preparations), organisations carrying out research and development of medicinal products, EU reference laboratories and digital providers. It obliges the EU Member States to adopt a strategic, comprehensive and collaborative approach to cyber protection, including by establishing national competent authorities and computer security incident response teams (CSIRTs) tasked with monitoring and analysing threats and incidents. In addition, EU-CyCLONe (EU cyber crisis liaison organisation network) is a supranational cooperation network for Member States' national authorities in charge of cyber crisis management to prepare for large-scale incidents.

[7] https://eur-lex.europa.eu/eli/reg/2019/881/oj
[8] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[9] https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf
[10] https://eur-lex.europa.eu/eli/dir/2022/2555

Importantly, senior managers overseeing the operations of entities deemed to be 'essential' or 'important' (the former being subject to a stricter regime, determined by the Member States) will be held personally liable for the implementation of technical measures and incident reporting. Both types will need to ensure cybersecurity staff training and to extend their own standards to their direct suppliers and service providers. Heavy sanctions will apply to non-compliant organisations. NIS 2 accompanies the 2022 *Directive on the resilience of critical entities*[11], which stipulates identification, risk assessment and resilience measures to be taken by Member States and the relevant selected entities, including in the healthcare sector.

In addition, the following three legislative files are currently under discussion:

- A targeted amendment to the Cybersecurity Act was proposed by the European Commission in April 2023 to enable the future adoption of European certification schemes for 'managed security services' such as incident response, penetration testing, security audits and consultancy.[12]
- The *Cyber Resilience Act*[13] *(CRA)*, proposed by the European Commission in 2022, goes beyond existing EU legislation on safety-related aspects of products and product liability by introducing mandatory and specific cybersecurity requirements for a broad range of products with digital elements throughout their lifecycle and hence primarily addresses manufacturers of hard- and software. Its provisions would enable purchasing managers of healthcare institutions and other end users (e.g., patients) to obtain appropriate information about the cybersecurity of the products they buy and use, with those classified as critical (e.g., operating systems, firewalls, central processing units, security elements) subject to third-party conformity assessments. Increased transparency and stringent manufacturer obligations are meant to ensure that relevant products placed on the EU market would have fewer vulnerabilities.
- The proposal for a Regulation on a *Cyber Solidarity Act*[14], published by the European Commission in April 2023, suggests common action to foster resilience against threats and incidents, thereby strengthening the link between EU security policies and the cybersecurity ecosystem. To detect and act upon cyber threats, the *Cyber Solidarity Act* proposes the establishment of a European Cyber Shield composed of national and cross-border Security Operations Centres (SOCs). The SOCs would make use of AI and advanced data analytics to detect and share warnings on threats and incidents, thereby allowing relevant entities to respond more effectively.

[11] https://eur-lex.europa.eu/eli/dir/2022/2557/oj
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454
[14] https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-cyber-solidarity-act

At the European Council level, 2022 saw the approval of conclusions on developing the EU's cyber posture[15] and adoption of the Framework for a coordinated EU response to hybrid campaigns, the latter reiterating that the continued development of the EU cyber posture is an important step towards preventing, discouraging, deterring and responding to malicious cyber activities as part of hybrid campaigns against Europe's security, while calling for a coordinated, multi-stakeholder response and application of the EU Cyber Diplomacy Toolbox.[16]

ENISA is closely linked to all components, and its role is bound to grow in importance over the coming years: under NIS 2, it will maintain a European vulnerability database (the agency is currently developing policies and procedures for its secure functioning), create a registry of service providers and publish biannual status quo reports; the CRA assigns information gathering, relay and incident mitigation tasks (e.g., proposing activities to be conducted by market surveillance authorities) based on notifications received from manufacturers of actively exploited vulnerabilities contained in products with digital elements; the Cyber Solidarity Act adds further responsibilities for developing cybersecurity skills and a European attestation scheme.

A new Joint Cyber Unit (JCU) has been created to support the implementation of the Cybersecurity Strategy, harnessing the expertise of various actors (grouped into the headings of resilience, law enforcement, cyber defence and cyber diplomacy) to pool their resources for providing mutual assistance. Although experts representing ENISA and EU-CyCLONe, the national CSIRTs and cybersecurity authorities are included under the 'resilience' stream, HOPE points out the need for closely integrating healthcare in the JCU's protection and coordination activities.

Other important cybersecurity-related actions at the EU level affecting individuals and public administration include the proposals for a legal framework for a European Digital Identity[17] (to enable secure use of public and private online services using mobile apps), the Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union and the EU Cyber Defence Policy.

In addition to legislative actions, several international and European standards (e.g., ISO, IEC, ETSI, CEN) and certifications are available on information security, privacy protection, cybersecurity and data exchanges offering guidance for procurers and managers of Health Information Systems[18]. Moreover, the NIST CSF[19] (National Institute of Standards and Technology CyberSecurity Framework), developed in the United States but internationally focused, provides a policy framework of computer security guidance enabling organisations to identify capabilities and gaps in their effort to attain cybersecurity compliance objectives.

[15] https://www.consilium.europa.eu/media/56358/st09364-en22.pdf
[16] https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281
[18] See ENISA's procurement guidelines for cybersecurity in hospitals, https://ec.europa.eu/futurium/en/system/files/ged/procurement_guidelines_for_cybersecurity_in_hospitals.pdf
[19] https://www.nist.gov/cyberframework

Implementation challenges

Making available adequate resources (financial, human, and organisational) will make or break European Union cybersecurity vision. In this regard HOPE notes with concern that, in the aftermath of the pandemic crisis, the global budgets of many hospitals and healthcare organisations across Europe remain volatile, making it difficult if not impossible for them to invest sufficient amounts in digitalisation and cybersecurity. While, under the 2019-2024 Multiannual Financial Framework, the EU is making available increasing amounts to support the implementation of activities described in the strategic documents listed above, notably making use of Digital Europe (including €375 million earmarked for cybersecurity out of €1.28 billion for the 2023-2024 period[20]) and Horizon Europe (2023 call for projects worth €50.7 million[21]) funding, additional financial support will be essential for the vision to turn into reality at the healthcare level to boost European, national and regional capacity.

Responding to the 2022 Council conclusions, the Cyber Solidarity Act foresees the establishment of a Cyber Emergency Mechanism, which is envisaged to cover preparedness actions (e.g., testing healthcare entities for potential vulnerabilities), the funding of an EU Cybersecurity Reserve (providers of incident response services), and make available financial support for mutual assistance. Total Cyber Solidarity Act funding will add up to over 1 billion EUR, 75% of which coming from the Digital Europe Programme.

Moreover, there is the challenge of adapting cybersecurity measures to particular organisations and their digital technologies. For example, the implementation of AI and robotics in hospitals represents a special cybersecurity challenge not only because of the wide scope of deployment covering many different areas (from medical imaging and diagnostics to health data recording, analysis and monitoring, surgical robots and disease-specific solutions, administrative and management tools, research and development) but because Europe's ambition to become a world leader is as much dependent on being able to collect, analyse and process vast health datasets as it is on building people's trust in data-driven technologies.

Featured among four reports released in June 2023 by ENISA is a discussion of the use of AI in medical imaging diagnosis of osteoporosis. It describes cybersecurity and privacy threats as well as vulnerabilities that can be exploited and concludes that, given the complexity of factors at play, "the entire cybersecurity and privacy context (requirements, threats, vulnerabilities, and controls) must be adapted to the context and reality of the individual organization".[22]

For hospitals, this ultimately implies the enormous and costly task of building up and maintaining a comprehensive cybersecurity architecture that covers all critical elements (IT applications and technologies, data centres, stationary and portable e/mHealth devices, telecom tools, terminals, etc.) and that can adapt to future technological developments and associated threats.

[20] https://digital-strategy.ec.europa.eu/en/news/eu13-billion-digital-europe-programme-europes-digital-transition-and-cybersecurity

[21] https://rea.ec.europa.eu/funding-and-grants/horizon-europe-cluster-3-civil-security-society/increased-cybersecurity_en

[22] https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-medical-imaging-diagnosis, p.51

HOPE is also concerned that the cybersecurity skills gap must be urgently addressed given the necessity to comply with complex and multilayered regulatory requirements which, coupled with the heightened threat landscape, calls for sufficient numbers of data and cybersecurity experts in healthcare[23]. Apart from the challenge presented by training qualified staff, which the European Commission proposal (released together with the Cyber Solidarity Act) for a Cybersecurity Skills Academy partially addresses[24], it will also be important to retain them. Given the shortage of cybersecurity specialists across sectors, more attractive salaries offered by private companies, and the general scarcity of health resources following years of underinvestment in many Member States, this will not be easy.

In summary,

- HOPE strongly supports making available additional EU funding to implement cybersecurity measures and ensuring that hospitals and healthcare institutions are able to benefit from comprehensive financial support so they can meet their multifaceted responsibilities.
- HOPE proposes that the Cybersecurity Skills Academy places a strong emphasis on skills development and education in the healthcare sector, ensuring that EU cohesion funds, the Recovery and Resilience Facility, InvestEU and other applicable EU programmes will be effectively used to boost cybersecurity know-how, leadership and expertise in the healthcare sector.

Meeting healthcare needs

Adapting cybersecurity measures and products as much as possible to the specific circumstances, needs and objectives of European health systems characterised by different national and regional service models, but nonetheless all handling particularly sensitive and private health data, is vital for ensuring that technological advances can be exploited securely and in harmony with healthcare providers' strategic goals and everyday operational requirements.

Moreover, it is critical to align EU cybersecurity measures with the expanding EU digital health architecture covering, inter alia, the proposal for a Regulation on a European Health Data Space (EHDS)[25], the proposed Artificial Intelligence (AI) Act[26,27], the Regulations pertaining to medical devices / in-vitro diagnostics, radio equipment, pharmaceutical legislation, etc., while respecting and promoting EU and national rules on data protection, ePrivacy and fundamental rights[28]. Until now, the primary focus has been on facilitating digitalisation rather than on cyber protection, with the EHDS as an essential vehicle for progress. It has been conceived to facilitate the EU-wide sharing of patients' health data covering both primary (healthcare, e.g. patient summary, electronic prescription and dispensation, laboratory results, hospital discharge reports, medical images) and secondary uses (health research, innovation, public policy).

[23] https://www.euractiv.com/section/cybersecurity/news/skills-gap-puts-eu-cybersecurity-rule-compliance-to-the-test/
[24] https://digital-strategy.ec.europa.eu/en/library/communication-cybersecurity-skills-academy
[25] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0197
[26] https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=CELEX:52021PC0206
[27] See also the June 2023 European Parliament briefing on the AI Act: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf
[28] As noted in HOPE's 2021 position paper on AI, https://hope.be/wp-content/uploads/2021/06/HOPE-Position-on-Artificial-Intelligence.pdf

That being said, the EHDS proposal also comprises wide-ranging security measures including security and interoperability criteria for Electronic Health Record systems, security audits for the MyHealth@EU and HealthData@EU infrastructures, robust authentication mechanisms for healthcare professionals and patients, and secure processing environments for secondary use purposes.

In this context, the intents of the Cyber Resilience Act (CRA) appear to be particularly relevant and appropriate, in legal and economic/social terms, and in response to calls by the European Parliament[29] and Council conclusions[30]. It provides an opportunity to define common cybersecurity standards while averting fragmentation, closing loopholes and addressing vulnerabilities that might otherwise not be detected.

HOPE welcomes the introduction of common essential cybersecurity requirements in the CRA, in particular obliging vendors to deliver 'security by default' by putting in place adequate safeguards and provide security information about a broad range of tangible and intangible digital products and ancillary associated services, including those (e.g., certain types of hardware, non-embedded software) not covered by existing EU legislation. Moreover, in healthcare, whole life-cycle requirements are valuable since technologies of different generations are often used in parallel. It will be fundamental to ensure that any product information provided is clear and understandable for its target audience.

Obliging third country vendors of connected products to comply with the CRA also presents an important opportunity to improve cybersecurity standards globally. Transparency builds trust in the safety and security of digital products and services, irrespective of their origin, and legal certainty for vendors.

Tying essential cybersecurity requirements to mandatory provisions on conformity assessments, CE marking and (post-)market surveillance is beneficial, not least given the limitations of self-assessments carried out by manufacturers and the blurred lines between functionalities and intended uses of different categories of digital products and services.

HOPE thinks that:

- Cybersecurity measures and solutions must take into account the fragmented nature of European health systems (e.g., regarding digital maturity and technologies deployed for specific purposes), as much as possible supporting ongoing transition processes and required system upgrades;
- The EU cybersecurity framework must be in full synergy with current and future EU legislation relevant to digital healthcare.

[29] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0286&from=EN
[30] https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf

Prevention and cyber hygiene

The best practice guides for the hospital and healthcare sector issued by ENISA[31,32,33,34] recommend establishing sector-specific CSIRTs, compliance with standards, staff training and awareness raising, and guidelines at the organisational level, coupled with network segmentation, asset and configuration management, monitoring and intrusion detection at the technical level. HOPE members also inform and share information about cybersecurity through dedicated networks and working groups; they encourage sectoral standards and educate management and staff about available tools[35]. Other HOPE members, in light of the shortage of cyber security skills, instead see advantages in working across sectors to make better use of scarce resources. However, a stronger, Europe-wide effort will be required to ensure all relevant actors are aware of their individual and collective cybersecurity responsibilities. It is also essential that sector-specific CSIRTs do not limit cross-sector and cross-border information sharing and cooperation. Responsibilities, functions and tools should be established to facilitate such cooperation.

Horizon 2020 projects CUREX, SPHINX and PANACEA produced tools for managing different phases of cyber-attacks, including software, methodologies, education kits, and guidelines enabling analysis of system security, risk assessment, threat intelligence, promotion of cyber hygiene and accountability.[36] The challenge is now to make sure these research results are promoted widely and that healthcare providers are able to access the catalogued solutions and afford their implementation.

Fostering individual responsibility is particularly difficult given the ubiquity of remote contacts individuals have via smartphones and other mobile devices, oftentimes mixing professional and personal uses. There is still a large knowledge gap regarding even basic security measures, from the selection of secure passwords to ensuring they differ for each device/account and are frequently changed. Hospital and healthcare staff at all levels needs to become fully aware that cyber-attacks can happen anytime and that each individual plays a part in preventing them. For health IT staff, secure configuration of end users' systems is paramount, i.e. disabling unnecessary applications, proper configuration of user accounts and protecting e-mail communication, deploying endpoint detection and response tools, securing backups, limiting Internet information and using minimal applications. Strong access control is also important, e.g. via two- or multi-factor authentication.

In addition, from an organisational perspective, it is also necessary to invest in various other measures, which might include developing an Information Security Policy, establishing IT document management systems, preparing business continuity and disaster recovery plans, and setting up risk management and compliance processes to address risks in a systematic way.

[31] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals
[32] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services
[33] https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services
[34] https://www.enisa.europa.eu/publications/csirt-capabilities-in-healthcare-sector
[35] An example from Belgium: https://www.santhea.be/CMS/content/images/202012/le-dfi-de-la-cyberscurit-dans-les-soins-de-sant.pdf
[36] https://digital-strategy.ec.europa.eu/en/events/how-european-funded-research-can-boost-cyber-resilience-hospitals

Therefore, HOPE proposes:

- actively involving HOPE and its members to sensitise European hospital and healthcare institution stakeholders to the challenges posed by cyber threats;
- ensuring relevant EU-funded cybersecurity research results, toolkits and solutions are promoted, accessible to, and used by hospitals and healthcare institutions; and, as a first step forward,
- placing particular emphasis on improving basic identification and authentication measures and skills, including use of secure passwords and more uniform procedures regarding the use of healthcare IT tools and systems.

****

HOPE, the European Hospital and Healthcare Federation, is a European non-profit organisation, created in 1966. HOPE represents national public and private hospitals associations and hospitals owners either federations of local and regional authorities or national health services. Today, HOPE is made up of 36 organisations coming from the 27 Member States of the European Union, as well as from the United Kingdom, Switzerland and Serbia as observer members. HOPE mission is to promote improvements in the health of citizens throughout Europe, high standard of hospital care and to foster efficiency with humanity in the organisation and operation of hospital and healthcare services.