SITRA

WORKING PAPER

7 MAY 2025

TOWARDS SAFER HEALTHCARE

Insights on the European action plan on cybersecurity for hospitals and healthcare providers

Markus Kalliola
Programme Director
Sitra

Mikko Huovila
Principal Consultant
Nordic Healthcare Group

Marianne Lindroth
Security Consultant
DNV Cyber

Europe's cybersecurity landscape is diverse and varied in maturity, making investment in healthcare cybersecurity essential for bolstering comprehensive security. The EU's cybersecurity action plan for hospitals and healthcare is a step forward in building resilience in Europe, with potential for further improvement through minor adjustments.

Sitra working paper

Towards safer healthcare – insights on the European action plan on cybersecurity for hospitals and healthcare providers

Authors:
Markus Kalliola, Sitra, Mikko Huovila, Nordic Healthcare Group and Marianne Lindroth, DNV Cyber

Sitra working group:
Teemu Linna, Andrea Rodriguez

Editor: Maria Nurmi

Layout: Grano Oy

ISBN 978-952-347-414-7 (PDF) www.sitra.fi
ISSN 2737-1042 (online publication)

Sitra working papers provide multidisciplinary information about developments affecting societal change. Working papers are part of Sitra's future-oriented work conducted by means of forecasting, research, projects, experiments and education.

Contents

Foreword

Europe is currently experiencing a transitional phase in terms of security. Russia's war of aggression in Europe and recent events in the US politics are causing uncertainty. This is not a temporary disruption in the security environment, after which there will be a return to the old normal.

Over the past year, Europe has been seeking answers to the changed security situation. In his report prepared for the European Commission, President Sauli Niinistö stated that the European Union needs to strengthen the preparedness and resilience throughout the society. Former President of the European Central Bank Mario Draghi also highlighted the importance of cybersecurity in his report focusing on the EU's competitiveness. European Commission President Ursula von der Leyen stressed the importance of cybersecurity in her political guidelines.

Cybersecurity is part of comprehensive security, and as society increasingly relies on digital services, its importance in organising critical services, such as healthcare, is emphasised. As part of strengthening Europe's comprehensive security, the European Commission unveiled an action plan in January 2025 to improve the cybersecurity of hospitals and healthcare providers. It aims to address growing cybersecurity threats and provide solutions that protect health data and ensure the functionality of information systems.

This working paper provides an overview of the action plan, cybersecurity regulations, and their impact on the healthcare sector. We will examine the current state of cybersecurity, challenges and opportunities, and present recommendations that can help improve cybersecurity in hospitals and among healthcare providers. Improving cybersecurity requires bold decisions and investments, but it is essential to ensure the functionality of healthcare even amid crises and individual disruptions.

Sitra, as an international future-oriented organisation, wants to be an active participant in the discussion on healthcare cybersecurity and in creating a better and safer future for Europeans. We hope that this publication will spark discussion and provide valuable insights for improving cybersecurity in healthcare.

We thank everyone who has participated in the preparation and commentary of this working paper. The recommendations are those of the authors and do not necessarily reflect the views of the advisory group or the experts who commented on the working paper.

7 May 2025

Markus Kalliola, Programme Director, Well-being solutions, Sitra

Summary

The healthcare sector is increasingly vulnerable to cyber threats due to outdated systems, fragmented practices and risks associated with human errors. Despite advancements in regulatory efforts and technical solutions, implementation remains inconsistent. Emerging technologies such as artificial intelligence (AI) and quantum computing add both urgency and complexity to securing healthcare environments.

The EU's expanding cybersecurity legislation is significantly impacting various sectors, including healthcare. The primary goal is to harmonise practices and enhance the resilience of critical entities, products and infrastructure. New instruments like the Directive on measures for a high common level of cybersecurity across the Union (NIS2), Cyber Resilience Act and AI Act broaden the scope of entities covered and introduce stricter requirements, raising the bar for compliance and emphasising the need for robust security in the interconnected digital landscape.

Europe has awakened to the need for taking further actions to protect healthcare. The European cybersecurity action plan for hospitals and healthcare providers, published by the European Commission in January 2025, arrives at a crucial time with several strong proposals to bolster healthcare security.

Sitra presents seven proposals for improving the preparedness of the EU and its member states against cyber threats. Building a single market for cybersecurity and making collaboration tangible through pan-European cybersecurity exercises are among the things to consider.

With all actions set to improve cybersecurity, clear targets are needed to measure the impacts. This applies to the Commission's action plan proposals for the EU and member states, but also at the grassroots level in healthcare organisations and how cybersecurity maturity is measured and improved.

Improving cybersecurity resilience requires healthcare organisations to address all stages of cybersecurity – before, during and after incidents. Cybersecurity should be further integrated into comprehensive security, with adequate resources allocated to healthcare organisations. A well-functioning single market is part of cybersecurity resilience, and European companies must play a significant role in it.

Finland serves as a case study for how cybersecurity is organised in healthcare within an EU member state. In Finland's comprehensive security model, cybersecurity responsibilities are distributed among various authorities. Healthcare organisations hold the primary responsibility, supported and guided by multiple authorities. Roles and responsibilities are clearly defined under normal circumstances, with the national cybersecurity strategy outlining priority actions.

Tiivistelmä

Terveydenhuolto on yhä alttiimpi kyberuhille vanhentuneiden järjestelmien, vaihtelevien käytäntöjen ja inhimillisten erehdysten vuoksi. Sääntelytoimien ja teknisten ratkaisujen edistysaskeleista huolimatta toimeenpano jää edelleen pistemäisiksi. Tekoälyn ja kvanttilaskennan kaltaiset uudet teknologiat edellyttävät ripeitä turvaamistoimia terveydenhuollon järjestelmissä samalla kun ne monimutkaistavat toimintaympäristöä.

EU:n laajeneva kyberturvallisuussääntely vaikuttaa perusteellisesti eri aloihin, myös terveydenhuoltoon. Sääntelyn tärkein tavoite on yhdenmukaistaa käytäntöjä ja parantaa kriittisten toimijoiden, tuotteiden ja infrastruktuurin kestokykyä kyberuhkia vastaan. Uudet säädökset, kuten Euroopan unionin kyberturvallisuusdirektiivi (NIS2), kyberkestävyyssäädös ja tekoälyasetus, laajentavat toimijoiden joukkoa ja asettavat tiukempia vaatimuksia, mikä korostaa vahvan tietoturvan tarvetta digitaalisessa ympäristössä.

Eurooppa on havahtunut tarpeeseen suojella terveydenhuoltoa ja ryhtynyt lisätoimiin. Euroopan komission tammikuussa 2025 julkaisema kyberturvallisuuden toimintasuunnitelma sairaaloille ja terveydenhuollon tarjoajille sisältää edistyksellisiä ehdotuksia turvallisuuden parantamiseksi.

Sitra esittää seitsemän suositusta EU:n ja jäsenmaiden kyberuhkiin varautumisen parantamiseksi. Esimerkiksi kyberturvallisuuden sisämarkkinoita on vauhditettava, jotta turvallisuuspalvelujen rajat ylittävä myynti helpottuu. Yhteistyötä on tiivistettävä järjestämällä Euroopan laajuisia kyberturvallisuusharjoituksia.

Kyberturvallisuustoimille on asetettava selkeät tavoitteet, jotta niiden vaikuttavuutta voidaan mitata. Tämä koskee komission EU:lle ja jäsenvaltioille osoittamia toimintasuunnitelmaehdotuksia sekä terveydenhuollon organisaatioiden kyberturvallisuuden mittaamista ja parantamista.

Terveydenhuollon organisaatioiden on parannettava kyberturvallisuuden häiriönsietokykyä ennaltaehkäisemällä kyberhyökkäyksiä, toimimalla tehokkaasti hyökkäysten aikana ja kehittämällä toimintaa hyökkäysten jälkeen. Kyberturvallisuuden tulee olla osa kokonaisturvallisuutta, ja terveydenhuollon organisaatioille tulee osoittaa siihen riittävät resurssit.

Suomi toimii esimerkkinä siitä, miten terveydenhuollon kyberturvallisuus on järjestetty EU:n jäsenvaltiossa. Suomen kokonaisturvallisuuden mallissa kyberturvallisuuteen liittyvät vastuut jakautuvat useiden viranomaisten kesken. Ensisijainen vastuu on terveydenhuollon organisaatioilla, joita useat viranomaiset tukevat ja ohjaavat. Roolit ja vastuut on selkeästi määritelty normaaliolosuhteissa. Kansallinen kyberturvallisuusstrategia määrittelee ensisijaiset toimet.

Sammanfattning

Hälso- och sjukvården blir allt sårbarare för cyberhot på grund av föråldrade system, varierande rutiner och mänskliga misstag. Trots att man gjort framsteg i fråga om regleringsåtgärder och tekniska lösningar genomförs åtgärder fortfarande inte genomgripande. Nya tekniker såsom artificiell intelligens och kvantberäkning kräver snabba åtgärder för att säkra hälso- och sjukvårdssystemen, samtidigt som komplexiteten i verksamhetsmiljön ökar.

Ökad reglering av cybersäkerhet inom EU påverkar olika sektorer i grunden, även hälso- och sjukvården. Regleringens viktigaste syfte är att harmonisera rutiner och förbättra kritiska aktörers, produkters och infrastrukturers resiliens mot cyberhot. Nya rättsakter såsom Europeiska unionens cybersäkerhetsdirektiv (NIS2), cyberresiliensförordningen och förordningen om artificiell intelligens breddar antalet aktörer och ställer strängare krav, vilket understryker behovet av stark informationssäkerhet i den digitala miljön.

Europa har vaknat upp och insett behovet av att skydda hälso- och sjukvården och vidta ytterligare åtgärder. Handlingsplanen för att stärka cybersäkerheten hos sjukhus och vårdgivare som Europeiska kommissionen lanserade i januari 2025 innehåller långsiktiga förslag för att förbättra säkerheten.

Sitra föreslår sju rekommendationer för att förbättra beredskapen på cyberhot i EU och medlemsländerna. Till exempel bör den inre marknaden för cybersäkerhet stimuleras för att förenkla den gränsöverskridande försäljningen av säkerhetstjänster. Ett närmare samarbete ska uppnås genom att man ordnar övningar i cybersäkerhet som omfattar hela Europa.

För att man ska kunna mäta hur effektiva cybersäkerhetsåtgärderna är ska tydliga mål ställas upp. Detta gäller de förslag till handlingsplaner för EU och medlemsländerna som kommissionen lagt fram samt mätning och förbättring av cybersäkerheten inom vårdorganisationerna.

Vårdorganisationerna ska förbättra cybersäkerhetens resiliens mot störningar genom att förebygga cyberattacker, fungera effektivt under attackerna och utveckla verksamheten efter attackerna. Cybersäkerheten ska utgöra en del av den totala säkerheten, och vårdorganisationerna ska tilldelas tillräckliga resurser för ändamålet.

Finland föregår som exempel på hur cybersäkerheten inom vården har ordnats i ett av EU:s medlemsländer. Enligt Finlands modell för den totala säkerheten är ansvaret för cybersäkerheten fördelad mellan flera myndigheter. Det huvudsakliga ansvaret ligger hos vårdorganisationerna som stöds och styrs av flera myndigheter. Rollerna och ansvarsområdena är tydligt fastställda under normala förhållanden. De huvudsakliga åtgärderna anges i den nationella strategin för cybersäkerhet.

1. Cybersecurity landscape in healthcare

The healthcare sector is facing rising cyber threats due to legacy systems, fragmented practices and workforce vulnerabilities. Regulatory framework is maturing, but implementation remains inconsistent. Emerging technologies like AI and quantum computing bring further complexity.

Growing attack surface and rising cyber threats

The healthcare sector is increasingly targeted by cyberattacks, with ransomware being a major threat that disrupts services and compromises patient safety. These attacks are often coupled with breaches of patient data, which often includes sensitive health-related data and violates people's fundamental right to protection of personal data. Nation-state actors engage in espionage and cyber disruption, aiming to steal sensitive data or weaken healthcare infrastructure. Cybercriminals target healthcare organisations for financial gain, leveraging stolen patient records for fraud or black-market sales.

Healthcare organisations store highly sensitive data, including personal identifiers, financial details and protected health information (PHI). The expansion of digital healthcare systems – such as electronic health records, telemedicine and Internet of Things (IoT) medical devices – introduces new vulnerabilities that attackers exploit. Supply chain risks increase as healthcare institutions depend on third-party vendors, cloud services and connected medical devices, such as monitoring systems that collect and transmit patient data. These interconnected systems have broadened the attack surface across the sector.

In Europe, the healthcare sector has been increasingly targeted by cybercriminals. For instance, in 2024, the European Union Agency for Cybersecurity (ENISA) reported 309 significant cybersecurity incidents affecting the healthcare sector, with ransomware accounting for 54% of these incidents between 2021 and 2023. These attacks severely disrupt critical services, including diagnostics and emergency care, and in some cases they have been linked to increased risks to patient safety.

Vulnerabilities of operational systems

Legacy IT systems in many hospitals lack modern security protections, making them easy targets. Software and hardware vulnerabilities are exploited through zero-day attacks and unpatched systems. Zero-day attacks are cyberattacks that exploit unknown software vulnerabilities before they are fixed, whereas unpatched systems are systems with known security flaws that have not been updated to fix those issues. Phishing and social engineering attacks remain prevalent, as healthcare employees often lack the skills to work in a way that ensures and enhances cybersecurity.

There are significant challenges related to the Internet of Medical Things (IoMT) in healthcare organisations. IoMT devices often have weak encryption and inadequate security protocols, making them vulnerable to cyberattacks. Robust cybersecurity measures are needed to protect these devices, including regular software updates, strong authentication

mechanisms and continuous monitoring. The potential impact of IoMT-related cyber incidents on patient safety and healthcare operations is substantial.

Endpoint complexity and fragmented governance significantly increase a hospital's risk of cyberattack. Hospitals must manage diverse, interconnected technologies – many acquired without central oversight – which introduces vulnerabilities across departments. As hospitals invest heavily in digital transformation, many still allocate only a small fraction of their IT budgets to cybersecurity. Meanwhile, many medical devices still lack built-in security and receive updates inconsistently across manufacturers.

Inconsistent coordination and fragmented implementation

A multidisciplinary approach is increasingly being recognised in practice as IT professionals, security experts and healthcare practitioners begin to collaborate more closely to mitigate cyber risks. However, coordination remains inconsistent across regions.

Governments, cybersecurity agencies, and private healthcare providers have taken initial steps to improve information sharing, but gaps in communication and threat intelligence dissemination still hinder a unified response. In addition to coordination challenges, cybersecurity still struggles to receive the level of prioritisation it requires compared to other urgent demands in healthcare operations.

While national and EU-level cybersecurity teams – such as computer emergency response teams (CERTs) and National Cyber Security Centres – have begun working together on incident response, the overall resilience against large-scale cyberattacks remains uneven and continues to evolve. The Cyber Solidarity Act promotes EU-wide collaboration, but real-time threat intelligence sharing is still limited. Some nations have more developed CERT teams, while others rely on outsourced cybersecurity firms, leading to variation in capabilities.

Many healthcare organisations have formal cybersecurity policies in place, yet they are not always clearly communicated or consistently understood by their staff. Incident reporting mechanisms exist, but underreporting remains a challenge due to unclear procedures or fear of repercussions. In many cases, dedicated cybersecurity teams are either understaffed or absent altogether, limiting the organisation's ability to respond effectively to threats.

Health sector burden and intrinsic risks

There are also specific and intrinsic risks to the healthcare sector. One of the most pressing is the high rate of personnel turnover, especially within human resources management. Staff changes challenge the implementation of long-term cybersecurity practices, making it difficult to maintain continuity and consistency. This is a sector-wide issue that exacerbates training gaps and the ability to enforce cybersecurity policies.

In terms of training, the challenges go beyond turnover. One of the largest hurdles is the limited amount of time available for healthcare professionals to participate in cybersecurity education. This limitation will become more critical as healthcare staffing shortages are projected to worsen in the coming years, further reducing the time available for preventive measures.

Awareness of cybersecurity risks among healthcare providers is gradually improving, with staff beginning to recognise common attack tactics used by cybercriminals, such as phishing and social engineering. Continuous education and training programs are being implemented in several EU countries, though participation rates and training quality vary.

Under the NIS2 Directive, mandatory cybersecurity training for healthcare

professionals handling critical systems is being rolled out, but compliance and integration into everyday operations remain in progress. High staff turnover is also visible among cybersecurity officers themselves, not just among the clinical personnel. This results in institutional memory loss and weakens continuity in cybersecurity governance, increasing organisational vulnerability over time.

Fragmented security adoption and slow transition

Some healthcare organisations have begun implementing stronger security controls, such as network segmentation and traffic monitoring to detect anomalies, as well as endpoint protection tools to defend against malware. Some institutions have begun adopting zero trust architecture (ZTA, a security model that assumes no user or device is trusted by default, enforcing strict access controls and continuous verification), though uptake varies widely across countries and is often limited by resource constraints. Regular security updates and patching are more common but delays still occur especially in legacy systems.

Large hospitals and national healthcare agencies conduct penetration testing and risk assessments. However, smaller healthcare providers often lack the financial and human resources to implement robust security protocols or carry out regular audits. Compliance is improving due to stricter regulations and financial penalties for breaches. General data protection regulation compliance is enforced, but data breach reporting remains inconsistent; the NIS2 enforcement is in early phases, and many healthcare providers are still adapting.

Third-party software and cloud services are often the weak points in security. Many healthcare organisations lack visibility into their vendors' cybersecurity practices. AI tools for automated threat detection and machine learning-based anomaly detection are being explored but are still in their early adoption stages. Progress is being made, but implementation remains fragmented and varies significantly across regions and institutions.

Critical technologies and the path ahead

Advanced technologies both increase risks and offer new means of defence. AI is increasingly used by cybercriminals for automating attacks, such as phishing and deepfake-driven fraud, requiring defenders to adopt more intelligent detection tools. At the same time, healthcare institutions are experimenting with AI-based anomaly detection and automated response, though deployment is limited to larger and better-funded organisations.

Quantum computing is emerging as a significant long-term concern. Once matured, it could break today's widely used encryption schemes, which would endanger the confidentiality of medical records and healthcare infrastructure. To mitigate this, standards for quantum-resilient cryptography are already being developed – the National Institute of Standards and Technology (NIST), part of the US Department of Commerce and the EU have released preliminary frameworks for post-quantum cybersecurity.

While proactive preparedness is widely recognised as a goal, many healthcare organisations still focus on incident response due to resource limitations. Recovery from cyber incidents often takes several days because of complex system dependencies, limited local capacity and fragmented preparedness across regions. Business continuity arrangements may fail under stress, especially in environments with insufficient ICT disturbance planning. This underlines the need for stronger regional preparedness frameworks and more systematic testing of resilience measures.

2. European Union's cybersecurity regulatory landscape and impact to healthcare

The EU's cybersecurity legislation is increasingly impacting the healthcare sector, introducing stricter requirements through instruments like the NIS2 Directive, Cyber Resilience Act and AI Act. The primary goal is to harmonise practices and strengthen the resilience of critical entities, products and infrastructure.

Directive on measures for a high common level of cybersecurity across the Union (2022/2555), NIS2

NIS2 expands cybersecurity requirements to new sectors beyond Directive on Security of Network and Information Systems (NIS1). In the healthcare sector, in addition to healthcare service providers, it now also includes the EU reference laboratories, organisations involved in the research and development of medicinal products, manufacturers of basic pharmaceutical products and pharmaceutical preparations, and critical medical device manufacturers during a public health emergency. Overall, NIS2 aims to harmonise cybersecurity requirements to safeguard critical infrastructure, such as hospitals.

The entities within the scope of NIS2 are required to identify themselves and provide the required information to the relevant national register. NIS2 categorises entities within the scope into two groups: important and essential entities. All entities considered critical entities under the Directive on the resilience of critical entities (2022/2557), will fall within the scope of NIS2 as essential entities, regardless of their size. Therefore, healthcare actors, are included in the scope of NIS2 as essential entities. They will be subject to a comprehensive ex ante and ex post supervisory regime and are also subject to more stringent fines than the important entities.

NIS2 mandates enhanced and broader risk management measures compared to NIS1. This includes an all-hazard approach to detect, assess, manage and mitigate the cybersecurity risks, ensuring business continuity through measures such as backup management and disaster recovery. Organisations must also have policies and procedures to assess the effectiveness of cybersecurity risk-management measures and ensure basic cyber hygiene practices and cybersecurity training.

In general, NIS2 continues and expands cooperation at the Union level. The EU-CyCLONe, a European cyber crisis liaison organisation network, is established to support the coordinated management of large-scale cybersecurity incidents and crises. The CSIRTs (computer security incident response teams) network is also responsible for collaborating and sharing information with the regional and Union-level security operations centres (SOCs) to enhance collective situational awareness of incidents and cyber threats throughout the Union.

Furthermore, NIS2 mandates a European network, the NIS Cooperation Group, to perform a coordinated security risk assessment, assessing both technical and strategic risks related to supply chains of ICT products, systems and services, including those related to medical device supply chains. Based on the assessment, they can propose mitigating measures. Additionally, while not directly

linked to NIS2, the Procurement Guidelines for Cybersecurity in Hospitals offers cybersecurity guidelines when procuring products, services and infrastructure, also providing procuring practices for hospitals.

NIS2 introduces stricter incident reporting within certain time limits. In addition, management bodies are required to undergo training to gain sufficient cybersecurity-related knowledge to be on top of the latest cybersecurity risks and best practices, which introduces an additional requirement compared to NIS1.

General Data Protection Regulation (2016/679), GDPR

GDPR is the most significant legislation covering the cybersecurity requirements, specifically in personal data processing within the European Economic Area. In the healthcare sector, it imposes strict security controls and requires appropriate technical and organisational security measures in the processing of personal data of the patients, customers, consumers, study cohorts, donors and other data subjects in the healthcare sector. This includes data minimisation, specified retention periods, the use of pseudonymisation and encryption measures, and the ability to detect a data breach, among others.

Furthermore, when applicable, data breach notifications must be submitted to the data protection authority, and in certain circumstances, the data subjects must also be informed.

Regulations on medical devices (2017/745) and in vitro diagnostic medical devices (2017/746), MDR and IVDR

The MDR/IVDR require manufacturers to develop products by implementing risk management principles, cybersecurity measures and conformity assessment procedures. Buyers of these devices may also wish to include these requirements in purchase contracts to emphasise the manufacturers' obligations.

The Medical Devices Coordination Group (MDCG) has issued a guidance in 2019 to support the implementation of the essential cybersecurity requirements. Currently, there is an ongoing evaluation of these regulations to improve the interplay of regulatory requirements in the field.

Cyber Resilience Act (2024/2847), CRA

The CRA aims to reinforce the Union's cybersecurity strategy and enhance cyber resilience at the Union level regarding products with digital elements, meaning software or hardware products and their remote data processing solutions. The act sets cybersecurity requirements for planning, design, development, handling, patching and reporting of actively exploited vulnerabilities in the hardware and software products involving digital elements. Accordingly, this is a significant regulation to address also in the healthcare sector product manufacturing, use and compliance, and may also include for example personal wearable products that include health monitoring features, designed to be worn or placed on the human body.

The act does not apply to certain products with digital elements already covered by other such existing rules. Accordingly, as stated in article 2 of the CRA, it does not apply to medical devices or any other products to which the MD and IVD regulations apply. The act entered into force on 10 December 2024, and it will be partially applicable from June 2026. However, most obligations under the act will be applicable from 11 December 2027.

Cyber Solidarity Act (2025/38), CSA

The CSA entered into force on 4 February 2025 and creates the Cyber Emergency Mechanism to enhance the preparedness and response to cybersecurity incidents by testing the potential weaknesses of critical sectors, such as healthcare. It also creates an EU Cybersecurity Reserve that consists of incident response services from private sector to support significant incidents, among others. A cross-border infrastructure of the European Security Operations Centre (SOC) will be part of a proposed European Cybersecurity Alert System which will improve the detection, analysis and response to cyber threats.

The healthcare sector will benefit from this act specifically through more coordinated, cross-border response capabilities for significant and large-scale incidents.

Artificial Intelligence Act (2024/1689), AI Act

The AI Act regulates the use of AI systems across different risk levels. Healthcare systems, such as medical diagnostics, patient care systems and medical devices, may include AI-powered systems which may fall within the scope of the AI Act.

From a cybersecurity point of view, the act imposes strict cybersecurity and transparency measures for AI-driven systems in healthcare. The act requires, for example, that providers of high-risk AI systems design and develop these systems to achieve an appropriate level of cybersecurity. Providers of such systems are required to equip the deployers with instructions for use, which must contain the level of cybersecurity and any conditions that may impact the level of cybersecurity.

Key EU cybersecurity regulations

Directive on measures for a high common level of cybersecurity across the Union (NIS2)

General Data Protection Regulation (GDPR)

Regulations on medical devices and in vitro diagnostic medical devices (MDR and IVDR)

Cyber Resilience Act (CRA)

Cyber Solidarity Act (CSA)

Artificial Intelligence Act (AI Act)

3. European action plan on cybersecurity for hospitals and healthcare providers

The action plan comes at a crucial time and has many good proposals to strengthen the security of healthcare. The main shortcomings are the lack of targets for actions which could be followed and measured. Also, the budget for implementing the action plan is not clear. The role of the private sector and the maturity, and the possibilities of a single market for cybersecurity are not covered in great depth.

The EU's security environment is rapidly changing, and it needs to strengthen the preparedness and resilience throughout society. President Sauli Niinistö raised this point in his report Safe Together, and Former President of the European Central Bank Mario Draghi also highlighted the importance of cybersecurity for competitiveness in his report. The European Commission President Ursula von der Leyen stressed the importance of the cybersecurity in its political guidelines and promised an action plan for hospitals and healthcare providers within 100 days since taking office.

The action plan was published in January 2025. It highlights the rapidly changing security environment in the EU, with an increase in hybrid attacks and cyberattacks targeting healthcare systems. The health sector has become the most attacked industry in the EU, particularly by ransomware gangs seeking financial gain from the highly valuable patient data.

Cybersecurity challenges

The action plan details the various cybersecurity challenges faced by hospitals and healthcare providers, including ransomware attacks, vulnerabilities in software and hardware and distributed denial-of-service (DDoS) attacks that, for example, maliciously direct traffic to a public health website causing it to crash. It emphasises the importance of securing digital health tools and data, which are crucial for improving patient care but also expand the potential targets for cybercriminals.

Cybersecurity maturity

The healthcare landscape in the EU is very diverse. The maturity of cybersecurity varies widely. The action plan finds deficiencies in key areas such as human resources, knowledge of ICT supply chains and installation of up-to-date security features. There is grave need for a culture of cybersecurity awareness among healthcare professionals.

European cybersecurity support centre

One key proposal in the action plan is establishing a dedicated European cybersecurity support centre within ENISA (European Union Agency for Cybersecurity) to support hospitals and healthcare providers. This centre would develop a comprehensive service catalogue, provide guidance on critical cybersecurity practices and facilitate the roll-out of national cybersecurity exercises.

Preventing, detecting, response and recovery of cybersecurity incidents

The action plan outlines measures to prevent, detect, respond and recover from cybersecurity incidents. It proposes the development of a regulatory mapping tool, a framework for cybersecurity maturity assessments and procurement guidelines. It also emphasises the importance of training and skills development for healthcare professionals. To detect cyber threats, the action plan introduces an EU-wide early warning subscription service for the health sector and the support of the European Health ISAC (Information Sharing and Analysis Centre) with tools and information exchange. It also suggests building a European known exploited vulnerabilities (KEV) catalogue for medical devices and electronic health record systems.

The action plan highlights the need for a rapid response service as part of the EU Cybersecurity Reserve to manage significant cybersecurity incidents in healthcare. It also proposes the development of cyber incident response playbooks tailored for healthcare and the facilitation of ransomware recovery subscription services.

To deter cyber threat actors from attacking European healthcare systems, fostering cross-border investigations is proposed as well as using the Cyber Diplomacy Toolbox to respond to threats.

National actions

The action plan does not solely focus on actions which the European Commission will take but also encourages member states to act. They should designate National Cybersecurity Support Centres for hospitals and healthcare providers and create national action plans focused on cybersecurity in the health sector. It also suggests facilitating resource sharing among healthcare providers and setting non-binding benchmarks for cybersecurity funding.

Public-private cooperation

The action plan discusses public-private cooperation and consultation with healthcare providers and cybersecurity industry players. It proposes the establishment of a joint health cybersecurity advisory board to advise on impactful actions and the launch of a call for action for cybersecurity companies to pledge support for the health sector.

Analysis of the action plan

The EU action plan covers well the current EU actions and proposes new measures which will greatly benefit the cybersecurity for hospitals and healthcare providers. The topic is timely and hopefully many of the planned actions will be completed successfully.

One central theme of the action plan is to increase collaboration in EU. The establishment of a cybersecurity support centre in ENISA and European Health Chief Information Security Officers (CISOs) Network are good examples. However, there are multiple other instances already collaborating in cybersecurity.

The EU-CyCLONE is a cooperation network for the national authorities of member states in charge of cyber crisis management. The CSIRTs network is another example that aims for an effective operational cooperation among the member states. The European Cybersecurity Certification Group was established by the cybersecurity act and among other functions it facilitates the cooperation between national cybersecurity certification authorities. Medical Device Coordination Group (MDCG) has a subgroup for new technologies and it advises member states also on cybersecurity.

There is a NIS Cooperation Group Workstream on Health which provides guidance to the member states on the implementation of the NIS Directive. ENISA is actively pursuing the EU Health ISAC (Health Information Sharing and Analysis Center) to provide situational awareness around

cybersecurity. Finally, the EU has an official agency for cybersecurity, The European Cybersecurity Competence Centre (ECCC), which aims to increase Europe's cybersecurity capacities and competitiveness, working together with the Network of National Coordination Centres to build a strong cybersecurity community.

Certainly, there has been a rationale behind the establishment of all the aforementioned networks. The new cybersecurity support centre and the CISOs network also have a good purpose. But, how do all the networks function as an entity and what is their cost-benefit ratio? The European Commission and the member states should simplify the governance and reduce the number of separate bodies and networks which facilitate cyber security among healthcare providers. The focus should be on adding value to healthcare providers who de facto implement cybersecurity activities and manage digital risks.

One significant shortcoming in the action plan is the lack of concrete targets for actions which could be followed and measured. The table at the end of the action plan lists all actions and their estimated due dates, but for example the plan of creating pilots does not present how many pilots will be launched and what their budget will be. Similarly, the plan aims to carry out annual health cyber maturity assessments but with no target on how many hospitals or healthcare providers or even member states would go through the assessment. The European Commission should define clear targets and budgets for each proposal in the next version of the action plan. The Commission has stated that it will be published by the end of 2025.

Finally, the action plan would benefit if it was linked to the EU's competitiveness, therefore having more emphasis on the cybersecurity industry and single market. The Draghi report stated that the EU is lagging behind in the field of digital technologies including cybersecurity. The EU innovation activities are primarily concentrated in sectors with medium to low R&D intensity, and especially the lower private R&D spending is the main reason for the EU's R&D spending gap. The European Commission should add actions to support the private sector R&D spending and actions to accelerate the selling of cybersecurity services across borders to build a cybersecurity single market.

Annex 1 includes an individual analysis of each action plan proposal.

Recommendations to improve the EU's action plan on cybersecurity for hospitals and healthcare providers

1. The European Commission and the member states should simplify the governance and reduce the number of separate bodies and networks which facilitate cyber security among healthcare providers.
2. The European Commission should define clear targets and budgets for each proposal in the next version of the action plan.
3. The European Commission should add actions to support the private sector R&D spending and actions to accelerate a cybersecurity single market.

4. How to improve Europe's cybersecurity resilience in healthcare?

It is essential in improving cybersecurity resilience that healthcare organisations consider all stages of cybersecurity – prevention, detection, response and recovery. Cybersecurity should be seen as part of comprehensive security, and healthcare organisations need enough resources to build and maintain it. But cybersecurity is not the responsibility of the public sector alone. European Union should step up and develop a strong single market with European cybersecurity companies taking a more active role in it.

Cybersecurity is one component of broader comprehensive security

Cybersecurity should be seen as part of the concept of comprehensive security. Comprehensive security involves ensuring that society's vital functions are handled in collaboration with the public sector, private sector and citizens. The basis of comprehensive security is that the arrangements, roles and functions of different actors of society are defined under normal circumstances.

Traditionally, cybersecurity has been seen as specific to organisations or partly sectoral. However, because of the changes in the security environment and because cyberattacks can be driven by malicious state actors and their proxies, cybersecurity should be considered a matter of national security. This leads to a major shift in positioning cybersecurity. Member states could consider calculating those parts of healthcare cybersecurity which relate to securing critical healthcare services into national defence expenditure.

Preparedness prevents threats to society's vital functions. It reduces the likelihood of threats and it is based on response needs. Response minimises the impacts of realised threats and promotes the recovery of society's vital functions. Healthcare cybersecurity should not be seen only as information security but as protecting healthcare services as a society's vital function.

Cybersecurity preparedness and response are essential to the resilience within healthcare. Good resilience produces security and trust in individuals, vital in a well-functioning society.

Healthcare organisations across Europe have significant differences in cybersecurity maturity. Because healthcare is organised in several different ways in the member states, the actors' ability to respond to cyber threats varies greatly. In general competence and resources are lower in smaller organisations. According to a recent survey by the Finnish Information Security Cluster (FISC), healthcare providers – particularly small and medium-sized organisations – consistently received some of the lowest scores for their cybersecurity maturity in the NIS2 sectors. FISC estimated that achieving compliance with just the NIS2 Directive and its national transposition law will require €100-200 million in investments across the Finnish healthcare sector.

Basic cybersecurity measures protect against most cybersecurity attacks. Up-to-date systems, backups and two-factor authentication

are straightforward to implement. All healthcare actors must attain a basic level of maturity in cybersecurity.

A tailored healthcare-specific maturity model for cybersecurity would ease the assessment of different organisations' preparedness. It would provide insights into weaknesses and the most efficient measures for improvement and it would be a functional instrument for directing funding.

Direct EU and national funding to healthcare organisations is a reasonable way to rapidly improve cybersecurity maturity. For the funding to be used appropriately, it needs to be targeted to activities that improve cybersecurity maturity according to the model. A shared maturity model should therefore be mandatory across Europe.

Single market for cybersecurity is the key to sustainable resilience

Security policy and cybersecurity are not just matters between the member states and the Commission, nor can cooperation with the private sector be resolved by establishing advisory groups and public-private partnership projects. The EU needs to build a genuine single market for cybersecurity and a unified operating environment for companies that create innovative cybersecurity services and products.

Our fragmented markets do not favour European actors. In the changed security environment, we cannot rely solely on security products from the US. This is not just about economic growth and jobs; either we build genuinely global and significant cybersecurity expertise or we fall into a cycle where declining competitiveness leads to protectionism and deeper technological dependence.

The healthcare cybersecurity market is large at the EU level but fragmented. A well-functioning single market is a significant possibility for European companies and a way to foster growth. Beside the policy level actions at the EU and member state level, there is a need for a general attitude change at the organisational level that every EU-based company is truly local. With that mindset, European-based growth companies can serve customers all over Europe. Beyond basic cybersecurity services the EU single market can give rise to special know-how and specialised, healthcare focused cybersecurity services which would not be viable in the current fragmented markets.

Preparedness investments produce long-term benefits

One key point in cybersecurity resilience is preparedness, which is related to maturity. Basic preparedness includes understanding the current state of the organisation's cybersecurity. These include cybersecurity and risk management, promoting cybersecurity culture and planning for information security violations and recovery.

In the healthcare sector, cybersecurity awareness is needed. Cybersecurity is not only technical competence but also organisational and professional development. Improving preparedness and cybersecurity requires determined long-term measures from professional education to robust adherence to cybersecurity standards.

Managers and staff need to understand the importance of cybersecurity and how their actions can affect threat prevention. This is a matter of education and leadership. The health sector has a lot of staff, and education should be as easy to access as possible. Cybersecurity skills should be part of healthcare professionals' basic education.

One way to improve preparedness is through cybersecurity standards. Although general cybersecurity standards are applicable in the healthcare sector, there are several challenges unique to healthcare. Patient safety, legacy systems, regulatory compliance, interoperability

and resource constraints are all factors that must be taken into account when standards are considered. Healthcare-related standards can expand requirements to sector-specific special issues. Cybersecurity standard certificates are one instrument for improving maturity.

Emphasis from theory to practise in the EU collaboration

Cybersecurity resilience requires strong cooperation between all stakeholders. Healthcare providers, authorities, the private sector and civil society need information exchange and shared situational awareness.

Smooth information exchange is required to construct shared situational awareness. This enables authorities, healthcare providers and private sector companies to cooperate effectively. The systematic gathering of information forms a comprehensive understanding of cyber threats in the healthcare domain.

Every member state should have a cooperation model between the key actors. Cooperation is based on shared situational awareness and the actors' ability to share information. Operational cooperation needs clear responsibilities for preparedness and responses to cyber threats. To work well cooperation also requires confidentiality and trust. The same information that is shared to prevent and prepare can also benefit malevolent actors, so it is essential to find practices where the actors can trust each other at national and the EU level.

Cybersecurity exercises are a practical way to advance cooperation. Security preparedness exercises allow healthcare organisations to test and develop cybersecurity operating models. These exercises help identify strengths and weaknesses in organisational operating models. One well-tested exercise model is tabletop practices which focus on organisational processes. The exercises are based on written materials and simulated situations.

Exercise activities are also essential for cooperation. Defined responsibilities will be tested when the key actors are involved in the same simulated cyber situations.

Exercise activities are beneficial not only at the organisational or national level; the EU should organise more EU-level exercises. Multi-country defence exercises between NATO countries serve as a good role model for what EU-level cybersecurity exercises should be. Multiple iterations of exercises would build practical capabilities and efficiency so that when organisations really need to work together during cyberattacks the collaboration would work in real life.

Recommendations to improve Europe's cyber security resilience in healthcare

1. Cybersecurity should be considered a matter of national security.
2. Cybersecurity maturity model for healthcare organisations should be mandatory and direct funding should be provided for improved maturity.
3. Cybersecurity skills should be part of healthcare professionals' basic education.
4. The EU should organise more pan-European cybersecurity exercises.

5. Case Finland: implementing cybersecurity in healthcare

In Finland's comprehensive security model cybersecurity responsibilities are divided among many authorities. The primary responsibility is always with the healthcare organisations, but many authorities guide and support them. Roles and responsibilities are clearly defined under normal circumstances.

Responsibilities of healthcare providers

Finnish healthcare is organised regionally between 21 wellbeing services counties, the City of Helsinki and HUS Group. In addition, there are private healthcare providers.

Healthcare organisations have the primary responsibility for cybersecurity. Finnish legislation defines cybersecurity responsibilities in the Act on Information Management in Public Administration and the Act on the Processing of Client Data in Healthcare and Social Welfare. General preparedness responsibilities are defined in the Act on Organising Healthcare and Social Welfare Services.

Healthcare providers are obliged to recognise cybersecurity measures and tasks that require exceptional reliability. Organisations must also organise instruction, education and cybersecurity supervision. In procurement processes, cybersecurity is required to be considered from the beginning to the end.

Organisations are also responsible for technical security, such as software maintenance, updates and integration security. Data logs, access rights and other data protection requirements are mandatory.

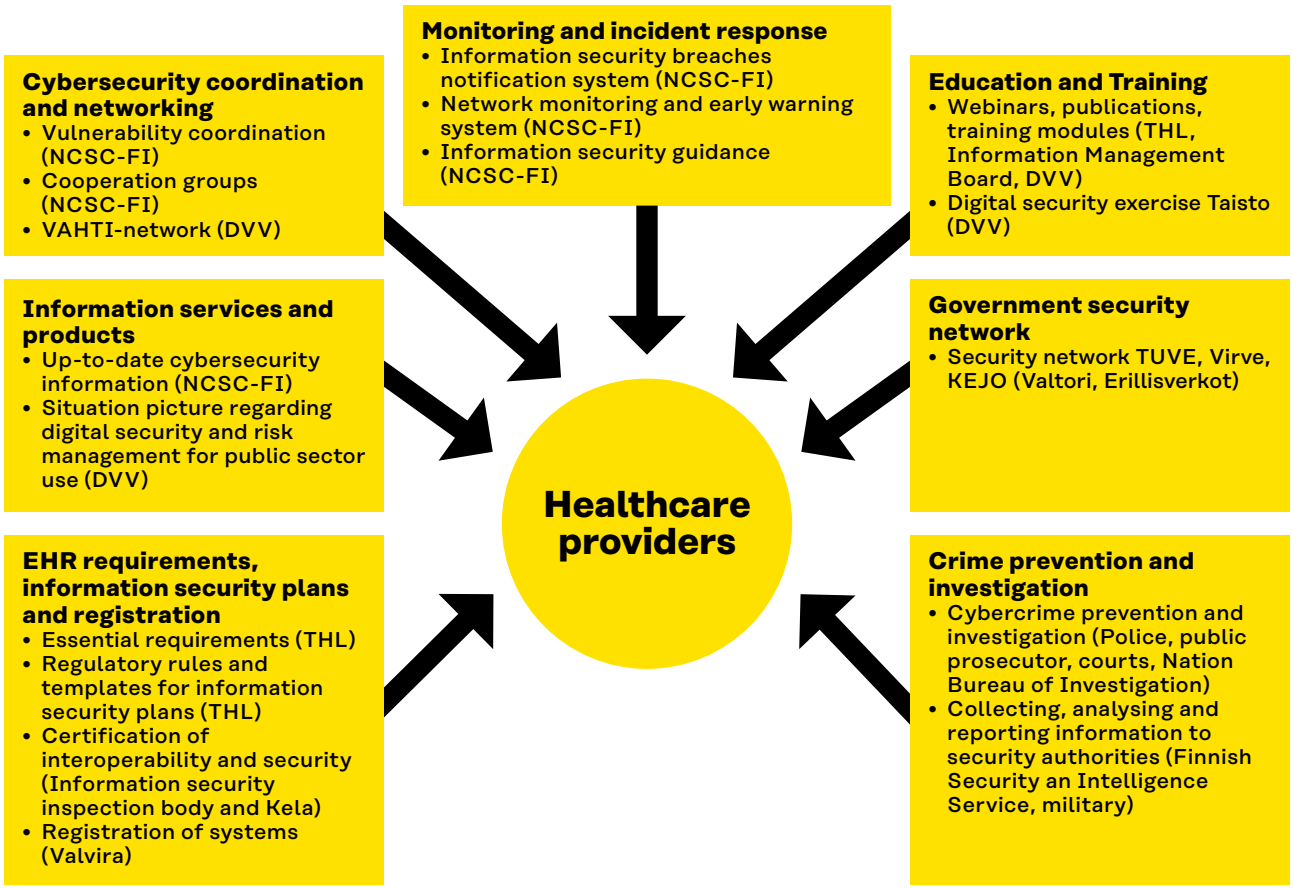
One central part of the legislation is preparedness and continuity management measures. Organisations are required to conduct risk assessments and implement proportionate information security measures. Incident preparedness, communication plans and tolerance testing are mandatory. Organisations should also have recovery plans and provide cybersecurity training.

Cybersecurity is one part of broader risk management and preparedness in healthcare. General risks include various pandemics and other disruptions in health security, use of military force, terrorist and other violent attacks, power supply disruptions, mass influx of migrants and chemical, biological, radiological and nuclear threats.

Wellbeing services counties oversee general preparedness and contingency planning in their respective counties. The wellbeing services counties operating a university hospital have five centres for preparedness in healthcare and social welfare. They coordinate and harmonise their respective counties' preparedness and contingency planning.

Guidance and support to healthcare providers

Figure 1. Authorities guide and support healthcare providers.



Healthcare providers get government guidance and support for various healthcare digitalisation and cybersecurity topics.

The essential requirements define the basis for the security and interoperability of electronic health record systems. Every EHR system must comply with these requirements. There is also a certification process and system registration. The National Institute of Health and Welfare (THL) provides the essential requirements. Informational security inspection bodies are responsible for security inspections.

The Social Insurance Institution of Finland (Kela) maintains national health data repositories (Kanta services) and are in charge of the interoperability testing. When the EHR systems pass the security inspection and interoperability testing, they are certified and registered to the national system register by the National Supervisory Authority for Welfare and Health (Valvira). Kela also has an information security supervision centre.

One way to support healthcare providers' cybersecurity responsibilities is through information security plans. These plans are statutory, and the National Institute of Health and Welfare (THL) provides the specific regulatory rules and templates. The idea of the plans is that they are used in daily service operations.

Information services also support healthcare organisations. Situation awareness products provide healthcare organisations with up-to-date information related to cybersecurity. These products include vulnerability reports, cyber weather reports, newsletters, articles,

alerts and an annual information security review. The National Cyber Security Centre produces these services.

Public sector organisations are given informational products that help them monitor the state of digital security and obtain related comparative information. The Digital and Population Data Services Agency collects ongoing information from public organisations to produce an overview of the situation regarding digital security and risk management for public sector use. This helps allocate resources to digital security development and support efficiently. The agency also surveys citizens' know-how, attitudes and experiences about digital security.

Cybersecurity coordination and networking are the principal ways to support organisations. This includes vulnerability coordination, information sharing groups, interference cooperation groups, critical infrastructure cooperation groups and information standardisation groups. The National Cyber Security Centre coordinates these groups.

The Digital and Population Data Services Agency is responsible for VAHTI, a network of organisations responsible for developing and steering cyber and digital security as well as experts in this field. VAHTI includes the management board for digital security in the public administration, three working groups and a network for central government information security responsible persons.

The National Cyber Security Centre offers monitoring and incident response services to detect information security incidents and supports organisations in these situations. Notifying the Cyber Security Centre about information security breaches helps the Centre assist private persons and organisations in resolving and investigating incidents and coordinating required actions. Network monitoring and early warning systems detect abnormal traffic. The National Cyber Security Centre also gives information security guidance for governmental organisations and critical infrastructure providers.

Organising education and training is essential in supporting healthcare organisations. This includes events, webinars, publications and training modules. The National Institute of Health and Welfare offers guidance, for example, on essential requirements, information security plans and access rights. The Information Management Board publishes recommendations about information security based on the Information Management Act. The Digital and Population Data Services Agency supports digital security at the general level by arranging events and publishing.

The digital security exercise Taisto is the largest cybersecurity exercise in Finland. It is a nationwide exercise that gives an opportunity to practise and develop digital security. This training event gathers hundreds of organisations from all sectors of society to prepare against current threats.

TUVE is the Finnish government security network. It secures the cooperation and communications of the government's executive leadership and the authorities that are vital to society's safety and security under all circumstances. For healthcare, the most critical services based on TUVE are Virve and Kejo. Virve is an authority radio network and time-critical broadband mobile communication service. Kejo is a system that allows authorities to cooperate – emergency care units use Kejo as an EHR. The government ICT Centre Valtori and the in-house company Erillisverkot are responsible for the TUVE services.

Crime prevention and investigation are the responsibility of the internal security authorities, the police, the public prosecutor and the National Bureau of Investigation. The Finnish Security and Intelligence Service collects, analyses and reports information to other authorities.

The Defence Forces also have cybersecurity duties when they are responsible for cyber defence and intelligence in the cyber domain.

The duties of the authorities in the cybersecurity field are gathered on next table.

Table 1. Cybersecurity responsibilities in the Finnish healthcare

Organisation	Responsibilities
Healthcare service providers	
Wellbeing services counties	• Primary responsibility for cybersecurity at the operative level • General preparedness and contingency planning
Wellbeing services counties operating a university hospital	• Coordinate and harmonise their respective counties' preparedness and contingency planning
Private service providers	• Primary responsibility for cybersecurity at the operative level
Health care specific	
Ministry of Health and Social Affairs	• Preparedness, readiness and cyber security strategic guidance
National Institute of Health and Welfare	• EHR essential requirements • Information security plan requirements • Overall health informatics guidance
National Supervisory Authority for Welfare and Health	• EHR registration • EHR supervision
Finnish Medicines Agency	• Medical devices supervision
The Social Insurance Institution of Finland (Kela)	• Maintains the Kanta services • Interoperability testing • Information security supervision related to the Kanta services and data communication
Public administration general	
Ministry of Finance	• Strategic and economic guidance of security network, ICT contingency planning, preparedness and security guidance
Digital and Population Data Services Agency	• Digital security development for the public administration
Information Management Board	• Promote the implementation of information management and data security procedures
Valtori	• ICT and integration services of the security network
Erillisverkot	• Security network and infrastructure services producing ICT services for the authority radio network and authorities' time-critical broadband mobile communications
Regional State Administrative Agency	• Preparedness and readiness supervision
Cybersecurity overall	
National Cyber Security Centre	• Develop and monitor the operational reliability and security of communications networks and services • Provide situational awareness of cyber security
Prime Minister's Office	• Finland's Cyber Security Strategy

Organisation	Responsibilities
Data protection	
Office of the Data Protection Ombudsman	GDPR and data protection compliance supervision
Supply processes	
National Emergency Supply Organisation	• Ensure the operating conditions of organisations that are critical to the security of supply
Internal security	
Police	• Investigate information network offences • National situational awareness concerning information network offences
National Bureau of Investigation	• Preventative operations
Finnish Security and Intelligence Service	• Collect, analyse and report information to other authorities
Defence	
Defence Forces	• Cyber defence and investigation

6. Next steps in making healthcare safer

Europe's cybersecurity landscape is diverse and the maturity varies. As part of improving Europe's comprehensive security, it is time to invest in cybersecurity and healthcare so that it is prioritised as a critical sector. The cybersecurity action plan for hospitals and healthcare is a good starting point, and with minor adjustments the European cybersecurity will be even further improved.

In recent years the EU has focused on setting a robust legal framework for cybersecurity. With the NIS2 and other new regulations there is no imminent need for new legislation. The time is now to invest into successful implementation of the regulations.

The healthcare provision is in the mandate of the member states, and therefore the EU's healthcare settings are country-specific. Also, the way cybersecurity is organised within healthcare is country- specific. This creates a paradigm: to raise the maturity in healthcare we need a single market for cybersecurity services and collaboration among countries. But, with each country having their national settings there is no "silver bullet" to make that happen.

The European cybersecurity action plan for hospitals and healthcare provides a good starting point for the discussion on how to make healthcare safer. In this working paper we have analysed the cybersecurity landscape, regulations, action plan and the national settings of one EU member state. In conclusion we will give seven main proposals to both improve the action plan, and in general increase resilience in healthcare:

Three main proposals for the European Commission to improve the action plan

1. The European Commission and the member states should simplify the governance and reduce the number of separate bodies and networks which facilitate cyber security among healthcare providers.
2. The European Commission should define clear targets and budgets for each proposal in the next version of the action plan to enable tracking of their success.
3. The European Commission should add actions to support the private sector R&D spending and actions to accelerate the creation of a cybersecurity single market.

Four proposals to add cybersecurity resilience to healthcare in the EU

1. Cybersecurity should be considered a matter of national security.
2. Cybersecurity maturity model for healthcare organisations should be mandatory and direct funding should be provided for maturity increase.
3. Cybersecurity skills should be part of healthcare professionals' basic education.
4. The EU should organise more pan-European cybersecurity exercises to ensure all the well-planned activities work in practice.

References

Alder, S. 2025. Healthcare Data Breach Statistics. HIPAA Journal.

Alder, S. 2025. The Ransomware Groups Targeting Healthcare Organizations. HIPAA Journal.

Coventry, L., & Branley, D. 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48–52.

Claroty. 2023. State of CPS Security Report: Healthcare 2023.

Council of the European Union. 2025. European Health Data Space: Council adopts new regulation improving cross-border access to EU health data. (accessed 25 March 2025)

Draghi, M. (2024). A competitiveness strategy for Europe. European Commission.

ENISA. 2023. Health threat landscape. European Union Agency for Cybersecurity.

ENISA. 2020. Procurement guidelines for cybersecurity in hospitals.

European Commission. (n.d.). Artificial intelligence in healthcare. (accessed 25 March 2025)

European Commission. 2024. Cyber Resilience Act. (accessed 25 March 2025)

European Commission. (n.d.). Data Governance Act explained. (accessed 25 March 2025)

European Commission. 2025. Directive (EU) 2022/2555: NIS2 Directive. EUR-Lex.

European Commission. 2025. European action plan on the cybersecurity of hospitals and healthcare providers. (accessed 25 March 2025)

European Commission. EU rules on medical devices and in vitro diagnostics – targeted evaluation. (accessed 20 March 2025)

European Commission. 2023. European strategy for data: Data Governance Act becomes applicable. (accessed 25 March 2025)

European Commission. 2024. New practical guide to the Data Governance Act. (accessed 20 March 2025)

European Commission. 2024. Regulation (EU) 2024/1689: Artificial Intelligence Act. EUR-Lex.

European Commission. 2024. Regulation (EU) 2024/2847: Cyber Resilience Act. EUR-Lex.

European Commission. 2025. The EU Cyber Solidarity Act. EUR-Lex.

European Parliament and Council of the European Union. 2016. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). EUR-Lex.

European Union. 2024. Regulation (EU) 2024/2847. EUR-Lex.

Europol. 2023. Internet Organised Crime Threat Assessment (IOCTA).

Finlex. 2018. Act 1050/2018 on the electronic processing of client data in health and social care.

Finlex. 2023. Act 703/2023 on preparedness in social and health care [Suomen säädöskokoelma].

Finnish Government. 2025. Lausuntopyyntö luonnoksesta hallituksen esitykseksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain ja eräiden muiden lakien muuttamisesta (accessed 30 March 2025)

Finnish Information Security Cluster (FISC). 2024. Member survey on cybersecurity maturity in NIS2 sectors – Summary of findings.

Haukilehto, T. 2024. Cybersecurity management in healthcare: Policies, awareness and incident reporting. Acta Wasaensia. Vaasan yliopisto.

Hellstén, H. 2018. Cyber risk management in the Finnish healthcare sector. University of Tampere. Trepo.

IBM Security. 2024. Cost of a Data Breach Report 2024.

Jalali, M. S., & Kaiser, J. P. 2018. Cybersecurity in hospitals: A systematic, organizational perspective. Journal of Medical Internet Research, 20(5), e10059.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1–10.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. 2017. Cybersecurity and healthcare: How safe are we? BMJ, 358, j3179.

National Institute of Standards and Technology (NIST). 2023. Post-Quantum Cryptography. (accessed 30 March 2025)

Niinistö, S. (2024). Safer together: A path towards a fully prepared Union. European Commission.

Office of the Data Protection Ombudsman. (n.d.). Letter concerning data breach notifications (PDF in Finnish). (accessed 20 March 2025)

OECD. 2021. Good Governance for Critical Infrastructure Resilience. (accessed 30 March 2025)

Paananen, R. et al. 2024. Finland's Cyber Security Strategy 2024–2035. Prime Minister's Office.

Parliament of Finland. 2024. Government proposal HE 57/2024: Cybersecurity Act [Proposal document, p. 238]. (PDF in Finnish).

Parliament of Finland. 2024. Hallituksen esitys eduskunnalle. (PDF in Finnish).

Sosiaali- ja terveysministeriö. 2024. Hallituksen esitys sosiaali- ja terveydenhuollon järjestämisestä annetun lain muuttamisesta (valmius ja varautuminen).

Sosiaali- ja terveysministeriö. (n.d.). Secondary use of health and social data. (accessed 20 March 2025)

Sosiaali- ja terveysministeriö. 2024. Hallituksen esitys eduskunnalle laeiksi sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain ja eräiden muiden lakien muuttamisesta.

THL. 2024. THL:n määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista on julkaistu.

Tiedonhallintalautakunta. 2024. Suositus tietoturvallisuuden vähimmäisvaatimuksista. Valtiovarainministeriön julkaisuja 2024:19.

Vuorinen, S. 2019. Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille. Sosiaali- ja terveysministeriö.

Vosikas, I. 2021. Cybersecurity in Internet of Medical Things. Risks and Challenges. XAMK – South-Eastern Finland University of Applied Sciences. Theseus.

Annex 1: European action plan on the cybersecurity of hospitals and healthcare providers – a review of the proposed actions

The Commission:

ENISA Cybersecurity Support Centre for Hospitals and Healthcare Providers		Review (Excellent, Good, Average, Below average, No review)
Ensure appropriate resources for the Cybersecurity Support Centre. Work with the ECCC to launch pilot projects to develop best practices for cyber hygiene and security risk assessment, and to address the need for continuous cybersecurity monitoring, threat intelligence and incident response using state-of-the art cybersecurity solutions, for the development of the European Cybersecurity Support Centre's service catalogue.	2025	Good. It would be even stronger with some estimates on the budget and capacity to operate. Similarly, "pilot projects" is very ambiguous term. What does it really mean, who will implement the pilots and with what budget?
Preventing cybersecurity incidents		
In consultation with the NIS Cooperation Group, EU-CyCLONe and ENISA, explore identifying health as a sector for which support can be given for coordinated preparedness testing under the Cyber Solidarity Act.	Q1 2025	Excellent. Coordinated testing is very much supported. Even better would be coordinated exercises and scenarios to build EU cybersecurity defence capabilities.
Rapid Response and Recovery		
Together with ENISA, ensure the EU Cybersecurity Reserve includes a Rapid Response Service specifically for the health sector.	Q4 2025	Good. As the EU cybersecurity reserve has not yet been established, its operational capacity is difficult to estimate. When it comes to "trusted providers" that are private sector companies, it will be important to ensure that they have relevant experience in providing cyber security services for healthcare.

ENISA Cybersecurity Support Centre for Hospitals and Healthcare Providers		Review (Excellent, Good, Average, Below average, No review)
Public-Private Cooperation		
Supported by ENISA, set up a joint Health Cybersecurity Advisory Board.	Q1 2025	Average. It is not clear what the mandate of this Advisory board is and what impact the advice it gives will have. The proposal could be improved by giving the Advisory board a clear role. For example, to follow the implementation of the action plan, set targets and measure impacts and propose yearly adjustments to the action plan.
Launch a call for action for cybersecurity companies, foundations, educational institutions, and industry stakeholders to pledge actions to address the challenges in the health sector.	Q2 2025	Average. The proposal has good intentions, but how much impact will voluntary pledges have?
Deterring cyber threat actors		
Together with the High Representative, explore the use of Cyber Diplomacy Toolbox measures to prevent, discourage, deter and respond to malicious activities against health systems.	2025	Not in scope of the analysis.
Advance international cooperation against ransomware actors, notably in the International Counter Ransomware Initiative, working together with the High Representative.	2025-2026	Not in scope of the analysis.
Seek cooperation in the G7 Cybersecurity Working Group to strengthen the cybersecurity of the health sector	2025-2026	Not in scope of the analysis.
Next steps		
Launch comprehensive stakeholder consultations.	Q1 2025	N/A
Adopt recommendations to further refine the Action Plan.	Q4 2025	N/A

ENISA:

EU Cybersecurity Support Centre for Hospitals and Healthcare Providers		Review
Begin work to establish a European Cybersecurity Support Centre for hospitals and healthcare providers.	Q2 2025	Excellent. The proposal will have great potential if the support centre has good resources and a clear mandate to operate.
Develop a comprehensive service catalogue to be provided by the Cybersecurity Support Centre.	From Q4 2025	Good. The aim to develop "a user-friendly, easy-access repository of all available instruments at European, national and regional levels" will come in need as there are many networks, actors and agencies working in the field of cyber security. The support centre can probably cover well the EU and even national instruments which often align with the EU legislation. But knowing the wide range of actors in the member states and diversity of services provided in them, it is not certain that this proposal will reach the regional level instruments it promises to deliver.
Preventing cybersecurity incidents		
Issue guidance that highlights the most critical cybersecurity practices and aid healthcare providers in implementing them.	Q3 2025	Excellent. The most critical practises are the low hanging fruit. Raising the EU cybersecurity maturity should start from them.
In close collaboration with Commission and member states, develop a regulatory mapping tool.	Q1 2025	Good. The RegTech approach which makes regulation easier to understand and follow is very much needed especially with a great deal of new legislation entering into force in cybersecurity.
Develop a framework for cybersecurity maturity assessments specific to healthcare.	Q3 2025	Excellent. We need to measure and gain understanding of the maturity. A common framework used throughout Europe will be a very good starting point.
Carry out an annual Health Cyber Maturity Assessment.	2025-2026	Average. The proposal would be better if it had targets of how many assessments will be completed and who would be targeted.

EU Cybersecurity Support Centre for Hospitals and Healthcare Providers		Review
Collaborate with member states and regional programme authorities to create Cybersecurity Voucher model programmes.	2025-2026	Average. The proposal would be better if the use of vouchers were coordinated. For example, raise the maturity level within the most critical cybersecurity practises, thus leveraging from the low hanging fruits. If the use of vouchers is not coordinated it will be hard to measure their impact. As the funding is not thoroughly discussed in the action plan, it is hard to place this proposal in a comparison with potential other funding options. Would a voucher model add bureaucracy compared to adding funding to the Digital Europe Programme in a targeted cybersecurity call for the same organisations which the voucher model would be offered? In principle new funding schemes should be avoided if the same impact can be achieved through existing means.
Develop new procurement guidelines for cybersecurity of hospitals and healthcare providers.	Q3 2025	Excellent. Procurement is a challenging task for the public sector. Increasing the maturity of actors throughout Europe in procurement might also help to grow the single market in cybersecurity. Private sector companies would have it easier to bid cross-border procurements if requirements were more aligned.
Create a European Health CISOs Network.	Q1 2026	Average. There are already a lot of networks, boards and agencies in the field of cybersecurity. Does one more in health add value? Does this network take resources from other proposals which might have more concrete results?
Design and promote training modules and courses for healthcare professionals.	Q1 2026	Good. Training of professionals in cybersecurity skills is very much needed. The proposal would be better if it included actionable steps on how the courses are delivered to the healthcare professionals and if it were clear whose responsibility it is. Also target values of how many professionals will undergo the trainings. When designing modules and courses a clear separation should be made between overall cybersecurity skills and organisational cybersecurity skills. Common training should focus on overall skills. The workforce in healthcare has a high turnover rate and often also temporary/contract labour is used. Therefore, having better generic skills for healthcare professionals will help each organisation to focus on their specific systems and needs. The training would be best placed already during studies or early in career.

EU Cybersecurity Support Centre for Hospitals and Healthcare Providers		Review
European capabilities for detecting cyber threats against the health sector		
Build up a European KEV catalogue for medical devices, electronic health record systems and providers of ICT equipment and software in health.	Q4 2025	Good. According to the US based Claroty's State of CPS Security Report: Healthcare 2023 report, 63% of known exploited vulnerabilities tracked by CISA are on healthcare organisation networks, and 23% of medical devices have at least one known exploited vulnerability. Therefore, there is a clear need for a KEV catalogue. The catalogue will work best when it collects data from existing sources and makes it easily available for the cybersecurity responsible persons at healthcare organisations. Relying on voluntary industry involvement to build the catalogue the results are likely to be less successful.
Introduce an EU-wide early warning subscription service for the health sector.	As of 2026	Good. If well-executed this could be a very useful service. The design should be done so that organisations that already subscribe to the national CSIRT notifications or other notifications, on which the EU service is based, do not receive double notifications. Furthermore, the alerts sent by the service must be customisable and selectable so that the user receives only the alerts they need.
Support the European Health ISAC with tools and information exchange.	2025-2026	Good. Industry collaboration is much needed, and this is one of the proposals where the public and private sector are doing just that.

EU Cybersecurity Support Centre for Hospitals and Healthcare Providers		Review
Rapid Response and Recovery		
Together with the Commission, ensure the EU Cybersecurity Reserve includes a Rapid Response Service specifically for the health sector.	Q4 2025	Excellent or Below average. The EU cybersecurity reserve established in the Cybersecurity Solidarity Act is composed of trusted private companies that are ready to assist the EU countries in the event of a major cyberattack. It is not clear what the action plan proposes regarding the rapid response service. If the plan is to make sure that the trusted private companies include companies with experience in health, the proposal is excellent. The health sector is unique, and companies with experience and focus on it can serve the sector better. But if the proposal is to build capacity in the newly established ENISA support centre, then it is a parallel activity to the CSA response service and as a proposal below average.
In collaboration with the CSIRTs Network, develop cyber incident response playbooks tailored for healthcare.	Q3 2025	Excellent. A playbook to support response and recovery is a good proposal. Especially when it also helps the organisation, under a cyberattack, to also utilise the services provided by the rapid response service and other EU-provided services which are probably not well-known for the health organisations.
Facilitate a large roll out of national cybersecurity exercises to test the playbooks and strengthen incident response protocols.	As of Q4 2025	Good. Practical exercises are very much needed. The proposal would be even better if it had targets of how many exercises are expected and what is the role of the support centre in them.
Provide a ransomware recovery subscription service.	As of 2026	Good. Similarly to other subscription services proposed, the service should be designed to complement national subscription services to avoid duplication.
Together with Europol, identify the most common ransomware strains targeting healthcare organisations and expand the repository of decryption tools through the No More Ransom project.	Q4 2025	Below average. As this is an already-ongoing activity by multiple organisations, public and private, and ENISA is already a partner in the project, it is difficult to see what the new added value of this proposal would be.
Together with Europol, develop accessible guidance to help healthcare providers avoid paying ransoms.	Q3 2025	Good. The health sector has specific data, and guidance for ransoms should consider the sector specific aspects – especially operational disruption and regulatory compliance.

EU Cybersecurity Support Centre for Hospitals and Healthcare Providers		Review
National Actions		
Assist member states in developing national action plans.	2025	Excellent. Especially the part where ENISA will ensure that European-level resources and practices are effectively used is very welcome.
Coordinate efforts to ensure that resources and strategies of individual member states complement each other.	2025-2026	Below Average. The argument that there is a need for increasing bargaining power towards cybersecurity service providers is a signal of immature markets where competition is not functioning properly, and for that reason the prices are high. To fix this a single market where competition is efficient and the price point is pushed to a reasonable level should be emphasised, not collaborative negotiation tactics.
Implementing and monitoring the Action Plan		
In consultation with the Commission, regularly provide updates of the work of the Cybersecurity Support Centre to relevant networks of member states.	2025-2026	Excellent. Updates are needed. Targets and budgets need to be clear and impacts measurable.
Continually exchange with the Health Cybersecurity Advisory Board.	2025-2026	Average. The added value of another advisory board is not clear.

Member states:

European capabilities for detecting cyber threats against the health sector		Review
Share incident notifications from hospitals and healthcare providers under NIS2 with the European Cybersecurity Support Centre	As of Q4 2025	Average. While this proposal is understandable, the reality of the NIS2 Directive is that majority of the member states have failed to address the deadline to transpose the Directive in their national laws. Even complying with the current legally binding measures is still in progress. Adding new requirements at this point is not very likely to be successful. The action plan should focus on proposals that are more actionable and more likely to succeed.
Encourage the development of national health ISACs	2025-2026	Good. ISACs are public-private partnerships and to build better and more resilient Europe collaboration is needed.
Preventing cybersecurity incidents		
Within the NIS Cooperation Group, perform a coordinated security risk assessment, assessing both technical and strategic risks related to medical devices supply chains.	Q4 2025	Excellent. The NIS2 Cooperation Group should take health as one of the priority areas and conduct risk assessments to medical device supply chains.
Rapid Response and Recovery		
Roll out national cybersecurity exercises to test the playbooks and strengthen incident response protocols.	As of 2026	Good. Cybersecurity exercises are a good approach to strengthen competencies and find gaps in organisational readiness. The proposal would benefit from clear targets that could be followed.

European capabilities for detecting cyber threats against the health sector		Review
National Actions		
Designate National Cybersecurity Support Centres for hospitals and healthcare providers.	Q2 2025	Average. In larger Member States, designated support centres might provide added value, but in most member states this proposal would most likely play out so that the CSIRT established in the NIS would be assigned another role with no additional resources. Therefore, the success of this proposal is very much linked to how much resources the support centre would receive, and could there be for example direct Digital Europe funding for establishing them.
Create national action plans focused on cybersecurity in the health sector.	Q4 2025	Good. National action plans are very much needed, because most of the actions in cybersecurity would be done at national or organisational level. The national action plan proposal would be even better if it included mandatory maturity assessments. Budgeting should be part of the national plans.
Facilitate resource sharing among healthcare providers.	2025-2026	Average. While the intention is good, the justification of the proposal does not fix the single market which has deficiencies in the cybersecurity field. Actions which build a strong single market with strong European companies would better serve both the public sector organisations and security as a whole.
Set non-binding benchmarks and monitor funding targets aimed specifically at cybersecurity.	Q4 2025	Excellent. Benchmarking and monitoring is needed. But not only at national level but also at the EU level including the action plan activities.
Request healthcare organisations and other entities subject to the NIS2 Directive to report their intentions to pay ransoms.	Q4 2025	This proposal is not justified in the text. It is unclear what is expected of this action.

Members of the focus group

Perttu Halonen, Senior specialist, National Cyber Security Centre Finland at the Finnish Transport and Communications Agency

Antti Härkönen, Senior Officer, National Supervisory Authority for Welfare and Health (Valvira)

Tommi Kuukka, Chief Information Officer, Western Uusimaa Wellbeing Services County

Andrei Laurén, Senior Specialist, Ministry of Social Affairs and Health

Mikko Pitkänen, Director, Finnish Digital and Population Data Services Agency

Risto Rajala, Advisor, The Finnish Information Security Cluster

Peter Sund, Chief Executive Officer, The Finnish Information Security Cluster

Jukka Tahkokorpi, Privacy and Security Architect, TietoEvry

Teemupekka Virtanen, Senior Specialist, Ministry of Social Affairs and Health

The working paper and its proposals represent the views of the writers, and they do not necessarily reflect the views of the members of the focus group.

SITRA

SITRA WORKING PAPER 7 May 2025
Sitra working papers provide multidisciplinary information about developments affecting societal change. Working papers are part of Sitra's future-oriented work conducted by means of forecasting, research, projects, experiments and education.

ISBN978-952-347-414-7 (PDF) www.sitra.fi

SITRA.FI
Itämerenkatu 11–13
PO Box 160
FI-00181 Helsinki
Finland
Tel: +358 294 618 991
Sitra