Policy Recommendations for Connected, Data-Driven, and Resilient Healthcare in Europe



January 2025

Table of Contents

Executive Summary

The European healthcare system faces a series of connected challenges: an ageing population, medical staff shortages, budgets under pressure, unequal access to treatment in sparsely populated areas. Covid-19 has been a catalyst for most of these issues but has also come with one benefit: the digital transformation of healthcare has made huge progress in recent years.

Digitisation of health is no panacea but can help address some of these challenges. It can result in greater operational efficiencies and increased staff productivity but more importantly it can impact patient care for the better. The suggested policy recommendations aim to maximise the benefits of healthcare digitisation, whilst reducing its risks for the digital resilience of hospitals and healthcare providers.

These recommendations include:

Connectivity	• Authorise Wi-Fi operations in the upper 6 GHz spectrum and open the 3.4-3.8 and 3.8-4.2 GHz bands for private 5G networks • Develop connectivity funding programmes to support the digital transformation of key sectors and the rollout of high-performance networks
Cybersecurity	• Launch dedicated funding programmes for cybersecurity at hospitals • Encourage hospitals and healthcare providers to identify, mitigate risk and ultimately replace connected devices in their networks if they are no longer subject to software updates by their manufacturers
Digital resilience	• Encourage hospitals and healthcare providers to develop digital resilience action plans, with possible measures on ICT risk-management measures, resilience testing, addressing third party risks
Data & AI	• Ensure that citizens can access their Electronic Health Records from a unique platform • Review procurement guidelines, certification and regulatory requirements that de facto require data to be held on premise • Encourage the uptake of AI and AI-enabled technologies in healthcare
Digital skills	• Establish clear digital training criteria per position of responsibility in hospitals, based on specific skills required • Provide training and expert support to public procurement professionals
Sustainability	• Review the Digital Decade Targets 2030 to reflect sustainability horizontally • Ensure that EU and national funding for decarbonisation is made available to digital transformation projects that have a sustainability and carbon reduction impact
Healthcare everywhere	• Provide funding for small and easily replicable digital health projects in remote areas

Introduction

This paper aims to explore how innovative technologies can shape the future of healthcare. The digital transformation of healthcare is already impacting how care is delivered, with the rise in telehealth since the Covid-19 pandemic, and the provision of tools that allow a shift toward prevention, anticipatory care, and community-based healthcare.

Digital health brings potential for operational efficiencies at hospitals that reduce overall costs, for example allowing better in-patient flows and bed management. It also supports the productivity of healthcare staff when they are under time pressure. It can improve access to healthcare in rural and underserved areas and stimulate patient involvement in self-care.

Fundamentally, healthcare has the potential to become much more patient-centric thanks to digital technologies. Finally, data analytics and AI can revolutionise healthcare by enhancing the accuracy, promptness, and efficacy of understanding population risks, conducting medical trials, and diagnosing medical conditions.

Digital transformation of healthcare comes with challenges, including data security and privacy, interoperability of systems, digital literacy of staff and patients, and adequate connectivity infrastructure.

The suggested policy recommendations aim to maximise the benefits of healthcare digitisation, whilst reducing its risks for the digital resilience of hospitals and healthcare providers. The paper also showcases some of the exciting digital health projects developed by Cisco[1] to enhance patient care and the efficiency and sustainability of healthcare facilities.




[1] This paper includes references to Splunk case studies following its acquisition by Cisco in 2023

Advanced connectivity for digital healthcare

The availability of resilient, secure connectivity is a foundational element of the digital transformation of healthcare facilities. With the recent dramatic increase in digital imaging and telehealth and the growing deployment of IoT devices, hospitals increasingly need reliable, high-speed, high-capacity network connectivity. Reliable bandwidth is needed to support the storage, integration, and exchange of digital data across multiple clinical and facility systems and applications. The use of new sensory robots requires low-latency and high-capacity networks. Conversely, poor connectivity can have very negative impacts on operational efficiency and staff productivity, but also more importantly on patient care and outcomes.

If available in all areas of the hospital, wireless connectivity in particular can enable technology solutions to enhance the supervision of patients through sensing, monitoring and connecting. It can also enhance scheduling and bed management through real-time tracking and location services, as well as the location and tracking of other equipment within a hospital or care facility.

Wi-Fi is a key enabling technology for healthcare facilities. Wi-Fi 6/6E and upcoming Wi-Fi 7 and Private 5G solutions have the potential to revolutionise the future of healthcare. Going forward, we expect a boost in IoT development and the growing adoption of augmented and virtual reality use cases. For these technologies to be widely adopted across European healthcare facilities, high-quality connectivity is needed and will rely on additional spectrum: allocating the upper part of the 6GHz band for Wi-Fi indoor and opening the 3.4-3.8 and 3.8-4.2 GHz bands for 5G private networks will be key to respond to these needs.

Enough spectrum will also be needed so that hospitals and other healthcare facilities can deploy dense networks that have enough wide channels to support different visitor/patient and internal networks, so that visitors can be hosted separately from sensitive internal and medical systems.

Case studies

Wi-Fi connectivity powers a secure and personalised patient experience and enables patients to use their own devices for wayfinding and portal experience within care facilities. A live demo conducted by the Wi-Fi Alliance showcased how utilisation of the full 1200 MHz Wi-Fi in 6 GHz delivers the heightened throughputs and stringent latency needed for advanced augmented and virtual reality (AR/VR) applications that support medical education and training, such as immersive virtual anatomy visualisation for doctors and medical students. Wi-Fi 6E can efficiently serve dense environments such as classrooms and training seminars with hundreds of students and doctors.

Policy recommendations

- Allocate sufficient spectrum to reap the full benefits of Wi-Fi and Private/Local 5G: European regulators should promptly authorise Wi-Fi operations in the upper 6 GHz band and open the 3.4-3.8 and 3.8-4.2 GHz bands for private 5G networks.
- European countries to develop connectivity funding programmes to support the digital transformation of key sectors and the rollout of high-performance networks, in collaboration with the private sector.

Enhanced cybersecurity of hospitals and healthcare providers

Cyber-attacks on healthcare providers have an oversized impact due to the sensitivity of data involved and the potential impact on life and health if their services are disrupted. Malicious cyber actors do not hold back from taking advantage of their risk profile. In recent months and years, we have seen a steep increase in ransomware and data-related attacks on European hospitals. In a recent ENISA report, 54% of 215 reported cyber incidents among healthcare organisations over a 27-month period in Europe involved ransomware and 46% involved data-related threats, such as breaches of patient data (ENISA report, 2023). This has recently prompted the European Commission to prepare an Action Plan on the Cybersecurity of European Hospitals, due to be released early 2025.

The European healthcare sector faces several cybersecurity challenges:

Lack of sufficient funding for cybersecurity: The French Government reacted to this and launched a dedicated programme for cyber in hospitals in December 2023, promising to spend €250M by 2025 (and €750M by 2027). This is an example that should be replicated across other European countries.

Lack of cybersecurity skills: Hospitals cannot remunerate their cybersecurity teams at the same level as in the private sector, so attracting talent is a challenge. Beyond technical departments, according to a report by ENISA, 40% of healthcare organisations do not have a security awareness programme for non-IT staff.

Outdated infrastructure and software: In 2019, 71% of medical devices were running on obsolete or near-obsolete software . Patching and replacing legacy devices and software is inhibited in acute care environments, where system downtime can be catastrophic, and where specialised legacy applications may not work on newer operating systems. Having legacy solutions is not a problem in itself, but leaving them at risk when they are no longer supported creates huge issues. Security practices such as identity intelligence, network segmentation and device trustworthiness can help mitigate risks.

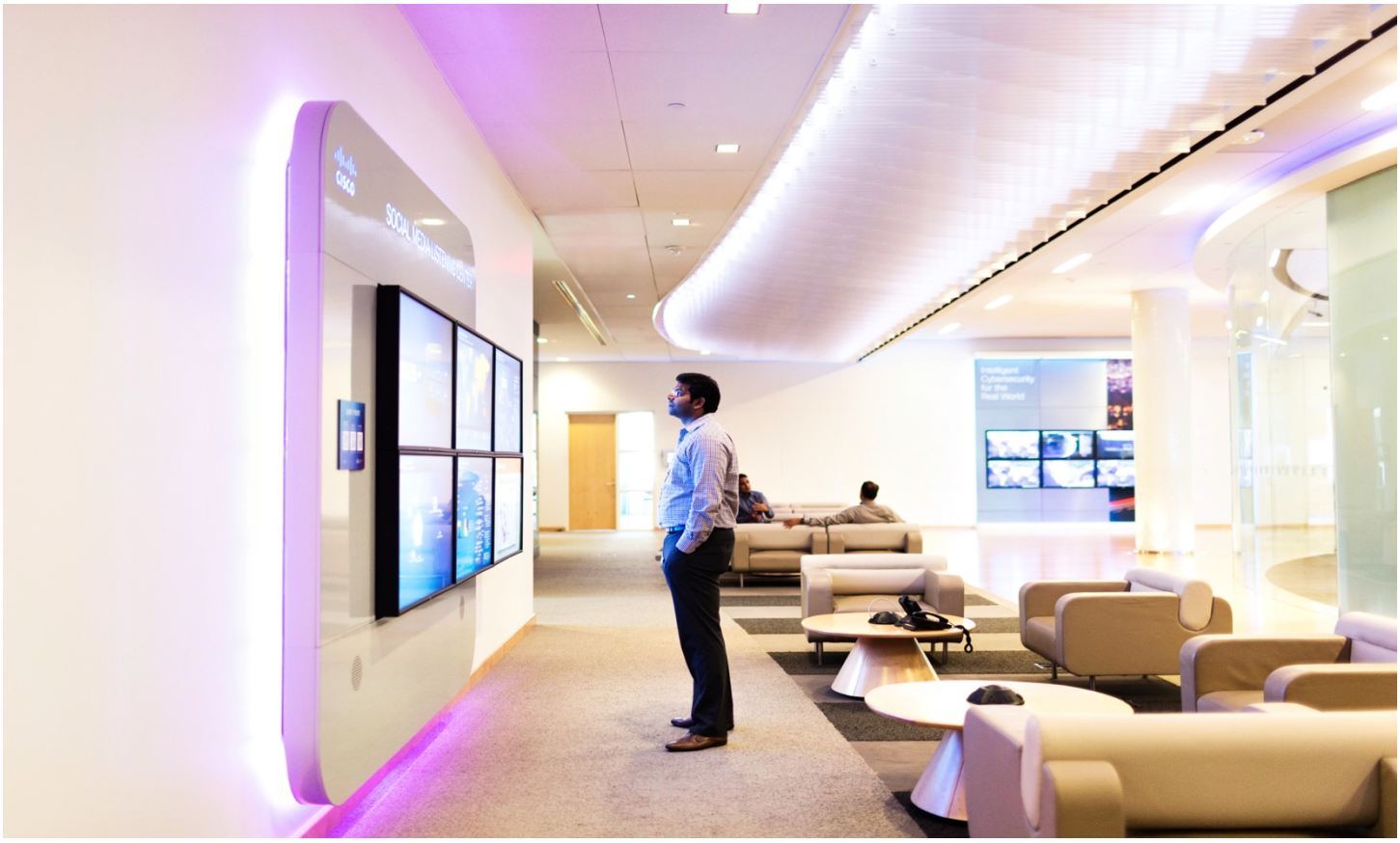
Lack of holistic and comprehensive risk-based cybersecurity strategies for hospitals (covering funding, skills, responsibilities, technology): Rather than relying on an overall strategy based on risk, hospitals tend to address cyber issues from a tactical perspective. To handle issues such as ransomware, they 'tick boxes' and buy additional solutions that create new siloes of technology, people, processes. Security is often an after-thought and a cost centre rather than an enabler for operational readiness and availability.

Case studies

In the State of New York, Cisco supported a large healthcare provider in overhauling its compute and storage infrastructure. Cisco Secure Workload helped establish a zero-trust environment, thereby enabling the organisation to manage and contain access to any server, application, or piece of data. As a result, they were able to map their applications and see all network traffic in real-time, streamlining monitoring and troubleshooting.

Policy recommendations

- Dedicated funding to be allocated to cybersecurity in hospitals as part of the next cybersecurity work plans of the Digital Europe funding programme;
- European governments to launch dedicated funding programmes for cybersecurity at hospitals, such as the CaRE plan in France;
- As part of the EU Action Plan on Cybersecurity of Hospitals, incentivise hospitals and healthcare providers to identify, mitigate risk and ultimately replace connected devices in their networks if they are no longer subject to software updates by their manufacturers;
- Member States to provide dedicated cybersecurity training for healthcare professionals, for example through national cyber agencies or other national cybersecurity fora (e.g. Campus Cyber in France).



Digitally resilient health infrastructure

Digitisation of health results in greater efficiencies and better patient experiences. With the growth in medical Internet of Things (MioT) and the proliferation of connected devices in a hospital environment, digitisation can, however, generate new vulnerabilities and cybersecurity attack vectors.

Some common security risks and vulnerabilities include weak authentication, lack of encryption, and outdated software. However, digital resilience goes beyond cybersecurity. A natural disaster or IT outage can have devastating consequences for critical infrastructure and continuity of care, as demonstrated by the CrowdStrike incident in July 2024.

A Splunk report issued in 2024 explored the "hidden costs of downtime" and calculated the average cost of downtime at $400B per year. Sectors are impacted in different ways. Whilst retail and manufacturing face the highest downtime costs, healthcare and public sector are also severely hit by downtime costs ($203M and $193M, respectively). This is without accounting for the broader non-monetary impact on patient health and wellbeing.

The key to digital operational resilience and to a strong cybersecurity posture is to have end-to-end visibility into all data and systems at all times. ICT risk management should be based on robust data analytics, to monitor and identify all sources of risks, detect anomalies and rapidly put in place response and recovery measures.

Case study

Centralised data analysis with Splunk increased visibility across StrongRoom AI's operations, which let its teams proactively monitor its IT infrastructure, troubleshoot performance issues, and maximise the uptime of its platform.

StrongRoom AI is a medication administration and management platform and a drug management solution that is used by more than 2,000 pharmacies, care facilities, and hospitals.

Policy recommendations

- European governments should encourage hospitals and healthcare providers to develop digital resilience action plans, with possible measures on ICT risk-management measures, resilience testing, addressing third party risks, etc. This should go beyond cyber risk-management measures.

Data-driven and AI-enabled healthcare

The potential of European health data remains largely untapped. Health data tends to be kept in siloes, with little to no data portability across hospitals and healthcare providers. For example, in Germany, hospitals have their own electronic patient records, creating a great deal of fragmentation. This siloed approach reduces the potential to use data to improve patient care and enhance diagnoses.

Effective data management requires integrating diverse data streams into a cohesive framework for secure and seamless access and sharing across different departments and/or external partners.

The EU has recognised this challenge by proposing the European Health Data Space (EHDS), which will introduce a common system of data governance and rules and guidelines for data exchange in the EU health sector. Given the great disparities across European health systems (which are centralised or regionalised) and the fragmented approach to the secondary use of health data, the implementation of EHDS will be a major effort that should only conclude towards the end of this decade. European hospitals are also not taking full advantage of cloud solutions, due to concerns around privacy and security of sensitive health data. Regulatory efforts to introduce guardrails that protect rights and mandate data governance, such as GDPR, or seek to remove barriers to transfer data offsite or across-borders, such as the EU Free Flow of Data Regulation, have failed to overcome this inertia, or even exacerbated it through overly strict interpretation. Primary patient data is held on-premises in many hospitals, limiting possibilities to adopt off-the-shelf solutions with modern feature sets, and to exploit the full potential of AI. A consequence of this is higher cost, less choice, and retention of legacy solutions that limit innovation and present a cybersecurity risk.

AI is often mentioned for its potential to improve diagnoses and patient treatments. In healthcare, AI can also greatly improve operational efficiency, by taking care of mundane tasks such as scheduling appointments or taking notes for doctors. These operational support tasks can reduce the administrative burden for healthcare professionals, who often complain about their time spent on paperwork.

Case studies

In Spain, Cisco partnered with Intel, Capgemini Engineering, Vodafone Spain, Gilead, and three hospitals to use AI and ML to improve the accuracy of COVID-19 diagnosis. Based on federated learning, an AI model trained by a large number of chest X-rays conducted in 3 hospitals was able to improve the accuracy of COVID-19 diagnoses and was also used to predict case severity.

Splunk supported the New York Presbyterian Hospital to address opioid diversion, a critical contributor to the opioid epidemic in the US. Using Splunk's data correlation and machine learning

capabilities, the platform immediately alerts the hospital if a physician prescribes a controlled substance to a patient who isn't in the care of the hospital, or if a pharmacy technician uses an automated dispensary cabinet more often than his or her peers.

Policy recommendations

- To prepare for the implementation of the European Health Data Space and build trust, EU Member States shall invest in capacity-building in their public administrations and in public awareness campaigns. Given the large investments that will be required to develop the necessary infrastructure, EU funding shall support national efforts.
- European Governments should also ensure that their citizens can access their Electronic Health Records from a unique platform, gathering data from across different providers. The EU has set a digital target of 100% of EU citizens having access to electronic health records by 2030, as per the Digital Decade Policy Programme.
- Subject to effective data privacy and security protections, European governments should review procurement guidelines, certification and regulatory requirements that de facto require data to be held on premise or otherwise impede healthcare providers' ability to adopt commercial off-the-shelf applications.
- In the EU, Member States and the European Commission should encourage the uptake of AI and AI-enabled technologies in healthcare, through specific pragmatic guidance on the use of these systems in the context of compliance with the AI Act, GDPR and the Data Act.

Equipping healthcare providers with digital skills

The health workforce is already under huge pressure, so digital skills training for staff is not always a priority. There is a major digital skills gap in the European healthcare sector, however, limiting technology adoption. The current curricula of health professionals do not reflect the skills required to navigate modern healthcare delivery.

In 2022, only 34% of healthcare workers reported having the workplace digital skills that they needed. Only 15% had experience using generative AI and only 14% said they possessed "advanced" knowledge of encryption and cybersecurity skills.

Digital literacy should also increase amongst patients if Europeans want to seize the opportunities of telemedicine and digital healthcare innovation. As part of the Digital Decade targets, at least 80% of the EU population should have basic digital skills by 2030. In 2024, only 55.5% of the EU population had reached that level, with great disparities across countries (from 27% to 82%).

Case study

In Ireland, Cisco's Networking Academy has supported 120,000 HSE (Health Service Executive) employees to advance their digital skills, especially in the area of cybersecurity.

Policy recommendations

- Member States to raise awareness and better prepare the population for career opportunities in digital health through information campaigns and appropriate training at different levels of the education system.
- For healthcare professionals, Member States should establish clear digital training criteria per position of responsibility, based on specific skills required, i.e.:
  - Cyber Resilience standard training for all healthcare staff
  - Cyber Lead Training for all Department heads
- As pointed out by DIGITALEUROPE in a recent paper[2], public procurement professionals in healthcare should also receive training and expert support to facilitate the procurement of appropriate digital solutions for health systems and institutions.

[2] DIGITALEUROPE recommendations for EU Digital Health Policy (2024-2029)

Smart and sustainable healthcare facilities thanks to digital technologies

Many European hospitals are old buildings in need of renovation. In the UK, an independent investigation of the National Health Service (NHS) mentions "crumbling buildings that hit productivity – services were disrupted at 13 hospitals a day in 2022-23. The backlog maintenance bill now stands at more than £11.6 billion. (...) .

Twenty per cent of the primary care estate predates the founding of the health service in 1948."

For hospitals, digital technology can be seen as a "fourth utility". A smart hospital can harness this 4th utility to deliver reduced power consumption, which leads to enhanced building operations, lower cost of ongoing operations, improved space and asset utilisation, and most importantly, reduction of carbon footprint.

In the UK, the Lister Alliance was set up to embed digital technologies seamlessly across the NHS, while testing new ways to deliver accessible, efficient, and personalised healthcare. Smart buildings is a key focus of the programme, and digital technologies are being tested for their sustainability benefits:

Smart lighting can improve patient and staff well-being "by mimicking natural daylight"[3];
Environmental sensors can improve energy management and reduce energy consumption, for example by "changing heating and ventilation levels in response to occupancy in a room";
Noise reduction can help create a better environment "for staff to work in and for patients to recover, working towards the ideal 'silent hospital'".

Case studies

Cisco technology can help with the sustainability and energy efficiency of hospital buildings. Cisco connects, powers and secures buildings. Connecting low-voltage Universal Power-over-Ethernet (UPoE+) provides security, connectivity, power, and observability. DC microgrids can make the buildings more energy efficient. By using DC power, healthcare facilities can reduce energy losses in the conversion from AC by more than 45%.

Cisco can orchestrate sequenced and intelligent automated control over software applications like the Electronic Health Records (EHR) with physical patient room devices such as lights, beds, blinds, and televisions. LED lighting, along with motorised shades, HVAC, and other systems can all be connected, programmed, powered, and secured with technology, which can now be considered to be the "fourth utility", alongside water, gas and electricity.

[3] all quotes from Lister Alliance website

Policy recommendations

- In the EU, review the Digital Decade Targets 2030 to reflect sustainability horizontally and enable sustainable digital transformation of hospitals.
- Make sure that EU and national funding for decarbonisation is made available to digital transformation projects that have a sustainability and carbon reduction impact.
- European countries should incentivise the digitisation of healthcare and healthcare facilities in programmatic documents, in particular by including infrastructure development as a key enabling factor and building upon the principles of the energy performance of buildings directive (EPBD).

Providing digital healthcare everywhere

Healthcare is a fundamental right for all of us. Yet, there are challenges around delivering healthcare in rural and remote areas. Shortages in healthcare professionals are exacerbated in these "medical deserts", where it is difficult to attract talent. Moreover, some people need to receive healthcare services at home for chronic diseases, long-term treatment and proactive prevention.

Telehealth enables caregivers and patients to be involved in self-care, is more cost-effective for public health spending and provides a better patient experience. Digital therapies can help increase patient access to treatment by reducing barriers (e.g. travel time to hospital, lack of specialised care available nearby), incorporating care as part of daily habit. However, the benefits of telehealth can only materialise if high-speed broadband is available at home, which can sometimes be a challenge in rural and remote areas.

Case studies

Ireland: Through its Country Digital Acceleration programme in Ireland, Cisco supported Home Health, a Digital Health trial on Clare Island, off the West coast of Ireland. This involves tracking vital signs via smart wearables, handling doctors' appointments via video calls and drones flying in prescriptions. Virtual reality headsets will also be used to deliver skills training for the nurses living on the island.

Germany: Together with several other partners, Cisco also launched the Medibus, a digital solution to close the healthcare gap across Germany and mobilise a state-of-the-art clinic in times of crisis. The solution provides all connectivity on the vehicle, cybersecurity and collaboration technology to power telehealth and translation services anywhere while managing all fleet operations remotely.

Policy recommendations

- European countries to provide funding for small and easily replicable digital health projects in remote areas (e.g. telehealth services provided in local pharmacies or townhalls). In the EU, Member States should boost connectivity in rural areas, with the support of EU funding (Connecting Europe Facility Digital; Cohesion Funds).

Conclusion

This paper aims to explore how innovative digitisation efforts should take a holistic approach in modernisation of today's and tomorrow's healthcare. As showcased above, connectivity, digital resilience, emerging technologies are all aspects of a multi-faceted challenge in supporting the digitisation of healthcare in Europe. Foundational to this aspect is that of the digital infrastructure, from a development, management and security perspective.

Europe's healthcare digitisation efforts can be as successful as the infrastructure they will have to rely on. The Digital Decade 2030 targets reflect significant challenges in obtaining a truly connected Europe, and the healthcare sector would be among the largest recipients of successful investments and growth in this space.

Policy Recommendations for Connected, Data-Driven, and Resilient Healthcare in Europe