Policy Brief

Digital Health Uptake

Data privacy and security in EU digital health

Guidelines for developers, enablers, and procurers

Authors: Raquel Costa-Almeida, Samuel Almeida, F6S Network Ireland

October 2024

Images: pexels.com; freepik.com

In cooperation with EU-funded Horizon Europe FOODITY project (grant agreement N° 101086105)

FOODITY

This policy brief examines the pivotal issue of data privacy and security within the European Union (EU)'s digital health sector. It outlines the current regulatory landscape, notably the General Data Protection Regulation (GDPR) and relevant directives, as well as the new EU Artificial Intelligence (AI) Act, and assesses their implementation across Member States. The brief highlights the persistent challenges posed by new technologies such as AI and IoT, as well as by increasing cyber threats that compromise patient data integrity and public trust. Addressing the need for uniform compliance and advanced security measures, it provides targeted guidelines for developers, enablers, and procurers of digital health technologies. The aim is to bolster privacy protections and security protocols, ensuring these innovations align with EU standards and effectively safeguard patient information across borders.

Defining digital health data privacy and security challenges in the EU

The rapid growth of digital health across the EU has heightened the need for robust data privacy and security measures that protect patient information and maintain public trust. With multiple stakeholders involved in developing, enabling, and procuring digital health solutions, clear guidelines are essential to ensure each party understands its role and responsibilities in safeguarding data. This policy brief presents practical data protection guidelines for developers, enablers, and procurers, providing tailored recommendations to support EU compliance, cybersecurity, and secure cross-border data sharing. By establishing a unified approach to data privacy, this brief aims to foster a secure, compliant, and interoperable digital health environment that respects patient rights and enhances collaborative healthcare innovation across EU Member States.

Roles defined. In the context of digital health data privacy and security, developers, enablers, and procurers each play distinct roles with unique responsibilities. Developers are responsible for creating digital health tools, applications, and devices that comply with EU privacy regulations, embedding security features and data protection measures from the start. Enablers—such as platform providers and infrastructure operators—facilitate the secure storage, transfer, and interoperability of health data, ensuring data privacy within their systems and alignment with EU standards. Procurers, including hospitals and government agencies, are responsible for selecting compliant vendors, assessing data protection protocols, and enforcing accountability in data handling practices. Together, these stakeholders contribute to a secure, integrated digital health landscape by addressing privacy and security from development through to implementation and data management.

EU context. The current landscape of data privacy and security in EU digital health is primarily governed by robust regulatory frameworks such as the General Data Protection Regulation (GDPR), which sets stringent standards for data protection across all sectors, including healthcare. Additionally, specific directives and regulations, such as the ePrivacy Directive[1] and the associated ePrivacy

[1] European Parliament, Council of the European Union. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Regulation, further delineate requirements for the handling of electronic communications and personal data.

In the EU, initiatives to certify and standardise digital health data systems are actively underway to improve data interoperability, quality, and security. A key development in this area is the European Health Data Space (EHDS), designed to create a unified framework for health data exchange across EU member states. The EHDS empowers individuals with control over their health data while enabling its secure use for healthcare delivery, research, and policy-making. Alongside the EHDS, the European Institute for innovation through Health Data (i~HD)[2] plays a critical role in promoting high-quality Electronic Health Record (EHR) systems across Europe. I~HD has led numerous projects focused on certification and quality labelling for EHR systems, ensuring they meet stringent standards and are interoperable across diverse healthcare environments. Collectively, these initiatives reflect the EU's commitment to advancing reliable, standardised digital health data systems that facilitate seamless healthcare delivery across borders.

Despite these comprehensive legal structures, the practical implementation of data privacy and security measures in digital health remains heterogeneous across Member States. This variability stems from differences in national laws that supplement GDPR, varied levels of technological adoption, and differing capacities of local healthcare systems to implement sophisticated cybersecurity measures. Furthermore, the increasing prevalence of cross-border digital health services exacerbates these challenges, demanding effective mechanisms for international data transfer and protection.

The rise of new technologies such as artificial intelligence (AI), big data analytics, and the Internet of Things (IoT) in healthcare also presents novel privacy and security concerns (see 'Challenges' below). These include issues related to data integrity, consent management for the use of personal data in AI algorithms, and the vulnerabilities introduced by interconnected devices.

The EU AI Act[3] is a landmark regulation setting comprehensive standards for AI use across sectors, including healthcare, to promote ethical, human-centred AI while ensuring safety, transparency, and fundamental rights protection. Passed on March 13, 2024, it introduces a risk-based classification system, with stringent requirements for high-risk applications such as digital health tools (DHTs). These include obligations for transparency, robustness, and oversight for developers and deployers. However, some ambiguities remain, particularly in aligning with sector-specific laws like the Medical Device Regulation (MDR). The Act's practical impact on digital health is still uncertain[4], as much depends on forthcoming implementation guidelines, standards, and adaptations by EU Member States. Regulatory sandboxes and other supportive frameworks aim to balance safety with innovation, supporting AI's ethical and secure integration across the EU's digital health landscape.

Challenges. One of the key challenges in ensuring data privacy and security in the digital health sector across the EU is the harmonisation of regulations and their enforcement across different Member States. Despite the robust framework provided by the GDPR, varying national implementations can lead to inconsistencies that may hinder effective cross-border data exchange and complicate compliance for digital health providers operating in multiple countries. Additionally, the rapid evolution of AI, big data analytics, and the Internet of Medical Things (IoMT) introduces complex risks including unauthorised data access, loss of data integrity, and issues with consent management, particularly when handling large volumes of sensitive health data. These technologies often outpace existing legal frameworks, creating a

[2] European Institute for innovation through Health Data, https://www.I-hd.eu/

[3] The EU Artificial Intelligence Act. Accessed 30 October 2024. https://artificialintelligenceact.eu/

[4] Stephen Gilbert, 'The EU passes the AI Act and its implications for digital medicine are unclear', npj Digital Medicine (2024)7:135.

gap between regulatory provisions and practical implementation. Furthermore, the increasing frequency and sophistication of cyberattacks targeting healthcare systems pose a significant threat, exploiting vulnerabilities in digital infrastructures and potentially leading to massive breaches of patient data. The challenge is not only technical but also involves fostering a culture of security and privacy that emphasises continuous risk assessment, employee training, and patient awareness. Ensuring robust data privacy and security thus requires a multi-faceted approach that adapts to technological advancements, strengthens regulatory alignments, and enhances cybersecurity measures within the health sector.

General guidelines to enhance data privacy and security

Developers, enablers and procurers need to navigate the complexities of data privacy and information security applicable to the EU digital health sector, including adherence to the GDPR and national data protection laws, regular security assessments. .Additionally, transparent handling of data and meticulous consent management are essential to maintain patient trust and compliance. Stakeholders must also focus on continuous user education to raise awareness about data security and engage actively with users to refine privacy features. Instituting a solid incident response plan, ensuring data integrity and availability, and using privacy-enhancing technologies are further critical steps. Moreover, adopting a risk management approach and securing cross-border data transfers with legal safeguards are crucial to managing the data lifecycle effectively. By embracing these practices, stakeholders can significantly bolster the security framework, fostering a reliable and trustworthy digital health environment across the EU.

Guidelines and strategic directions for developers

1. Security-by-design: Embed security from the outset of app, device, or software development. Use practices like data encryption, user authentication, and secure access controls.

- **Barrier:** Implementing "security-by-design" in AI-driven health tools is challenging due to limited resources, technical complexity, and regulatory clarity. Smaller developers especially face financial and operational challenges in meeting high compliance standards from the outset.

- **Proposed recommendations:** Encourage EU-funded training and grants to assist developers, especially SMEs, in embedding security features early in the design phase. Create accessible EU resources and certification pathways that standardise the security-by-design process, providing a clear roadmap for compliant development.

2. Data minimisation and anonymisation: Limit data collection to only what is necessary and anonymise data when feasible to protect patient identity.

- **Barrier:** Ensuring data minimisation and anonymisation in complex AI models is difficult, especially when these models require extensive datasets for training and refining.

- **Proposed recommendations:** Create specific data minimisation standards for different AI applications, allowing developers to comply with clear, structured guidelines that balance data privacy with model efficacy.

3. Compliance best practices: Ensure adherence to GDPR, including data portability, data deletion, and access rights. Employ frameworks to regularly review and update compliance measures.

4. Continuous security testing: Implement regular security audits and penetration testing

to detect vulnerabilities early and maintain a secure environment.

- **Barriers:** Continuous security testing and compliance monitoring add cost and complexity, especially for companies operating across multiple EU states with varied local interpretations of regulations.

- **Proposed recommendations:** Introduce centralised EU testing and compliance hubs where developers can test security features in line with pan-European standards. Encourage collaboration with notified bodies to streamline testing processes across borders, ensuring consistent compliance without redundant local testing.

Guidelines and strategic directions for enablers

1. Secure data storage and transfer: Use encrypted, secure data storage solutions, and establish protected data transfer protocols, ensuring compliance with GDPR and EHDS.

2. Interoperability standards: Ensure infrastructure supports data interoperability while adhering to EU standards, **facilitating safe and efficient cross-border data sharing**.

- **Barriers:** Maintaining secure, interoperable infrastructure that meets cross-border data-sharing requirements is complex, with variations in national security policies and technical standards.

- **Proposed recommendations:** Develop a unified EU framework for healthcare data interoperability that enablers can integrate, with security requirements and data-sharing protocols applicable across Member States. Promote partnerships with cybersecurity firms to establish a shared security infrastructure for health data.

3. Cybersecurity measures: Maintain rigorous cybersecurity practices, including firewalls, anti-malware protections, and intrusion detection systems to safeguard patient data.

- **Barrier:** High costs associated with implementing and maintaining rigorous cybersecurity measures can be prohibitive, particularly for smaller platforms and new entrants in the digital health market.

- **Proposed recommendations:** Introduce EU shared cybersecurity services for smaller enablers, lowering entry barriers while enhancing security across the board. Promote the use of open-source cybersecurity tools that meet EU standards, enabling cost-effective compliance with robust security protocols.

4. Backup and disaster recovery: Develop robust data backup and recovery plans to protect against data loss or breach, crucial for maintaining service continuity.

- **Barrier:** Lack of standardized disaster recovery protocols can lead to inconsistent response times and data loss in the event of a breach or system failure, affecting healthcare service continuity.

- **Proposed recommendations:** Standardise disaster recovery plans across EU nations, requiring enablers to adopt predefined recovery timelines and procedures. Establish EU certification for disaster recovery and mandate regular training for compliance, ensuring fast, effective response capabilities throughout the sector.

Guidelines and strategic directions for procurers

1. Privacy-first procurement: Use encrypted, secure data storage solutions, and establish protected data transfer protocols, ensuring compliance with GDPR and EHDS. Prioritise vendors and solutions with strong privacy and security credentials, ensuring compatibility with GDPR and EHDS standards.

2. Security due diligence: Assess vendors' data protection protocols, requiring documentation of compliance, security practices, and regular security audits.

- **Barriers:** Procurers face challenges in evaluating and comparing vendor data privacy and security standards, particularly with international or non-EU providers whose practices may not align with EU requirements.

- **Proposed recommendations:** Develop EU-supported vendor assessment frameworks that provide clear criteria for evaluating privacy, security, and compliance of digital health tools. Establish a certification registry of compliant vendors to simplify the selection process and ensure alignment with EU data protection standards.

3. Data processing agreements: Establish detailed data processing agreements with third-party providers, clearly defining data handling, access rights, and responsibilities.

- **Barriers:** Establishing effective data processing agreements (DPAs) with third-party providers is complex and often lacks standardized terms, which can lead to ambiguous data handling responsibilities.

- **Proposed recommendations:** Develop standardised DPA templates that outline minimum compliance requirements, including data access, handling, and breach notification protocols. Encourage the use of these templates across the EU, ensuring consistency and reducing legal complexity for procurers managing multiple vendor relationships.

4. Vendor accountability: Implement checks to monitor vendor compliance with privacy and security guidelines continuously, ensuring that third-party systems do not compromise patient data security.

- **Barriers:** Ensuring vendor accountability for ongoing compliance is challenging, especially for healthcare institutions with limited resources for continuous vendor monitoring.

- **Proposed recommendations:** Support EU-wide compliance auditing services that provide affordable, periodic checks on vendors' data protection practices. Encourage procurers to include contractual obligations for third-party audits, and implement EU guidelines for scalable, efficient vendor oversight processes.

Patient-centric data governance

Enhancing patient trust in digital health systems is crucial, and adopting a patient-centric approach to data governance plays a pivotal role in achieving this. By prioritising the autonomy and privacy of patients, healthcare organisations can foster a sense of security and confidence among users. This involves transparent communication about how patient data is collected, used, stored, and shared, ensuring that patients have clear, accessible information. Implementing robust consent management processes that allow patients to easily understand their choices and control their data is essential. Furthermore, providing patients with the ability to access, review, and manage their own health information can empower them, giving them a direct role in their healthcare management. Such measures not only comply with legal requirements like the GDPR but also go a long way in building trust. This trust is vital for the acceptance and success of digital health technologies, as it reassures patients that their most sensitive information is handled with the utmost care and respect, ultimately enhancing their willingness to participate in digital health initiatives. An example illustrating the effectiveness of patient-centric data governance is the EU's Horizon Europe FOODITY project[5] (details on lessons learnt are provided in the Annex).

Recommendations for cross-role collaboration

To create a cohesive and secure digital health ecosystem, cross-role collaboration is essential. **Unified compliance standards** should be established to help stakeholders align on

[5] https://foodity.eu/

privacy and security measures, creating a consistent and coordinated approach across the EU. By adopting **joint accountability models**, stakeholders can share responsibility for compliance, clearly defining roles and making enforcement of data protection easier and more efficient, particularly in cross-border contexts. To facilitate ongoing alignment, **collaborative platforms for information sharing** are beneficial to allow developers, enablers, and procurers to exchange best practices, compliance updates, and lessons learned, fostering a culture of adaptability and continuous improvement. Additionally, **training and awareness programmes** should be implemented collaboratively to strengthen understanding and adherence to data privacy and security standards. Such programmes can be tailored for each role, ensuring that all stakeholders possess the knowledge necessary to support and enforce robust data protection. Facilitating such training programmes and/or providing financial support to develop more robust digital data infrastructure and services is a priority for the upcoming years.

Recommendations at a glance

- A **robust policy framework** is crucial for achieving **uniform data privacy and security standards in digital health across the EU.** The development of EU-Level standards and certification programmes would provide stakeholders with a clear pathway for compliance with GDPR, EHDS, and other relevant regulations, ensuring a streamlined and consistent approach across all member states.

- To foster innovation and address the unique challenges of cross-border data security, the EU should **allocate funding for innovation in (cyber)security** — particularly for new tools, cybersecurity advancements, and adaptive technologies in the healthcare sector.

- **Resource allocation for capacity building** should target regional disparities by supporting smaller entities and underserved areas, helping them meet EU data security standards.
- **Streamlined regulatory guidance** would offer simplified, consistent information on compliance expectations, reducing complexity and enabling developers, enablers, and procurers to navigate data protection regulations with greater ease and clarity.

Together, these policies aim to foster a more secure, inclusive, and compliant digital health environment across the EU.

Concluding remarks

As the EU strives to enhance healthcare delivery through digital platforms, it is imperative to establish a robust framework that ensures the protection of sensitive patient information and maintains public trust. The implementation of EU-wide standards, along with certification programs and targeted funding for cybersecurity innovations, are crucial steps toward fostering a secure and compliant digital health environment. Looking forward, the continued evolution of technologies such as AI and IoT in healthcare will necessitate ongoing adaptations to these frameworks to keep pace with new developments and emerging threats. Moreover, fostering collaboration among all stakeholders — developers, enablers, and procurers — will be key to overcoming barriers and achieving a cohesive digital health ecosystem across the continent. By addressing these challenges with proactive and unified policies, the EU will strengthen their role in the global digital health sector, ultimately improving health outcomes for all citizens and setting a benchmark for digital health security internationally.

ANNEX

To illustrate the effectiveness of patient-centric data governance, the EU's Horizon Europe FOODITY project[6] (GA no. 101086105) offers valuable lessons in enhancing privacy and user control, providing a model from which digital health can greatly benefit. These lessons suggest that a balanced approach — integrating user empowerment, resource accessibility, collaborative frameworks, and strong EU support — can strengthen data privacy and security across digital health applications.

Lessons learned and best practices from the EU FOODITY project:

- **Data sovereignty and user control:** FOODITY centres on giving users complete control over their personal data. This focus highlights the importance of privacy-by-design and transparency in health data, ensuring users have clear rights to access, manage, and consent to the use of their data.
- **Interoperable and harmonised frameworks:** FOODITY demonstrates how standardised frameworks can drive data interoperability across diverse sectors and stakeholders, a critical need in cross-border health data sharing. This example underscores the benefit of harmonised EU-wide standards, supporting seamless data exchange while maintaining security and compliance across Member States.
- **Supportive infrastructure and resources:** FOODITY illustrates the value of EU funding and technical resources in lowering barriers to innovation. For digital health, similar EU-supported grants and open-source tools could help smaller developers and enablers implement robust security measures, particularly in resource-limited regions.
- **Multi-stakeholder collaboration:** By uniting stakeholders, FOODITY facilitates cross-sector alignment on data handling and compliance practices. Translating this approach to digital health could foster collaborative best practices, encouraging joint accountability and consistent privacy measures across developers, enablers, and procurers.

As part of the FOODITY Pilot Programme, it can also be mentioned the DIAITA project[7], funded under the first FOODITY open call. The DIAITA project aims to empower patients, caregivers, and healthcare professionals by providing them with science-based dietary recommendations and involving them in decision-making to adapt them to each patient's nutritional needs. The initiative ultimately aims to offer a practical, reliable, and transparent digital service that drives knowledge sharing and advances AI technology in healthcare. This is also well aligned with patience-centric data governance.

[6] https://foodity.eu/

[7] https://foodity.eu/meet-the-foodity-innovators-diaita/, https://www.youtube.com/watch?v=2wWHMWJMGL8