EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Procurement guidelines for the cybersecurity of hospitals and healthcare providers

JULY 2026

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use ehealthSecurity@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

European Union Agency for Cybersecurity (ENISA)

ACKNOWLEDGEMENTS

ENISA would like to thank the NIS Cooperation Group Workstream on Health, the EU Health ISAC, and the European Commission for their valuable contributions to the development of this report.

ISBN 978-92-9204-804-4, DOI 10.2824/2503342

Table of Contents

Executive Summary

According to the European Commission, there are over 500 000 types of medical devices and in vitro diagnostic medical devices available on the EU market, ranging from simple bandages to complex imaging systems and implantable devices ([1]). In 2023, the European medical technology market was valued at approximately EUR 160 billion, making it the second-largest market globally after the United States ([2]).

The increasing digitalisation introduces significant cybersecurity challenges, highlighting the urgent need for enhanced procurement practices that embed robust cybersecurity measures. The European Union Agency for Cybersecurity acknowledges cybersecurity as essential for ensuring the resilience of the health sector, particularly following the adoption of Directive (EU) 2022/2555 (updated Network and Information Security Directive, NIS2), which sets stringent security obligations, including procurement, for essential and important health entities.

The procurement guidelines presented in this document are intended to help hospitals and healthcare providers ([3]) integrate cybersecurity objectives into their procurement processes. Covering all phases of the procurement life cycle, they offer practical guidance for addressing cybersecurity risks in a comprehensive manner. The guidelines set out clear cybersecurity requirements, specify the necessary information that suppliers must provide, and are closely aligned with relevant regulatory frameworks such as the NIS2 Directive, the medical device regulations, the general data protection regulation and the European health data space regulation.

This guidance defines the three key procurement phases – plan, source and manage – and identifies the types of services and products where cybersecurity considerations are particularly important. It also highlights specific cybersecurity measures to be implemented, with a focus on supply chain security in the healthcare context.

The document concludes with a practical checklist of cybersecurity measures tailored for healthcare procurement. Each measure is linked to relevant procurement types and the specific threats it helps mitigate, and the checklist is designed to be easily filtered. To illustrate how these measures can be applied in real-world scenarios, three hypothetical use cases are provided: the procurement of medical devices, the procurement of cloud services and the procurement of off-the-shelf Electronic Health Record (EHR) system from a general practitioner.

([1]) European Commission, ‘Overview’, European Commission website, https://health.ec.europa.eu/medical-devices-sector/overview_en?utm_source=.

([2]) Fortune Business Insights, ‘Europe Medical Devices Market’, Fortune Business Insights website, 26 January 2026, https://www.fortunebusinessinsights.com/europe-medical-devices-market-107576.

([3]) ‘Healthcare provider’ means ‘any natural or legal person or any other entity legally providing healthcare on the territory of a Member State’ (Article 3(g) of Directive 2011/24/EU of the European Parliament and of the Council). Examples include emergency medical services, digital health service suppliers, medical device manufacturers, logistics suppliers, pharmaceutical companies and public authorities.

1. Introduction

Healthcare services across Europe are undergoing significant transformation, enabled by the integration of digital technologies and the widespread adoption of connected medical devices. This evolution is further supported by Directive (EU) 2022/2555 – the updated Network and Information Security (NIS2) Directive – which aims to enhance the cybersecurity and resilience of critical infrastructure, including the health sector. The transformation spans a broad spectrum of stakeholders, including hospitals, emergency medical services, cloud-based and software-as-a-service digital health suppliers, medical device manufactures and electronic health record (EHR) systems vendors, logistics and supply chain entities, insurance companies, pharmaceutical organisations and public authorities.

This digital integration brings forth significant cybersecurity challenges. The European Union Agency for Cybersecurity (ENISA) has identified the health sector as particularly vulnerable to cyber threats. According to the *ENISA Threat Landscape 2024* ([4]), the health sector accounts for 8 % of total ransomware incidents, making it one of the most affected sectors. This high exposure is attributed to factors such as the widespread use of legacy systems, limited cybersecurity budgets and the complexity of healthcare supply chains. Notably, the 2022 edition of *NIS Investments* reported that only 27 % of healthcare organisations have a dedicated ransomware defence programme, while 40 % lack security awareness programs for non-IT (information technology) staff ([5]).

In 2025, the European Union has intensified its efforts to enhance the cybersecurity and digital resilience of the health sector through several strategic initiatives. A cornerstone of this effort is the European Commission's action plan on the cybersecurity of hospitals and healthcare providers, launched in January 2025 ([6]). The plan focuses on four key pillars: prevent, detect, respond and deter, and it calls for the development of updated procurement guidelines for hospitals and healthcare suppliers, building on the 2020 ENISA guidelines ([7]).

This document was prepared by ENISA, in collaboration with the European Commission and the NIS Cooperation Group. A review process was initiated by ENISA in collaboration with the European Commission and the Member States.

1.1. Objective

This guidance aims to provide comprehensive cybersecurity procurement guidelines for hospitals and healthcare providers across various service segments, for example emergency medical services and electronic health record systems' suppliers, cloud-based digital health service suppliers, medical device manufacturers, logistics suppliers, insurers, pharmaceutical companies and public authorities.

1.2. Scope

This guidance addresses the entire healthcare ecosystem, acknowledging the complexity of defining cybersecurity requirements across diverse healthcare services. The recommendations cover both

([4]) ENISA, *ENISA Threat Landscape 2024 – July 2023 to June 2024*, 2024, https://data.europa.eu/doi/10.2824/0710888.
([5]) ENISA, *NIS Investments – November 2022*, 2022, https://data.europa.eu/doi/10.2824/433214.
([6]) https://ec.europa.eu/commission/presscorner/detail/en/ip_25_262.
([7]) ENISA, *Procurement Guidelines for Cybersecurity in Hospitals – Good practices for the security of healthcare services*, European Network and Information Security Agency, 2020, https://data.europa.eu/doi/10.2824/943961.

organisational and technical cybersecurity measures and specify the required security documentation and evidence suppliers must provide for their network and information systems ([8]) and services.

While the NIS2 Directive does not directly impose requirements on information and communications technology (ICT) suppliers ([9]), its obligations take effect through national laws that transpose the directive into domestic legislation. As such, this guidance does not override or replace any national regulations, and healthcare providers should ensure that they comply with the specific legal requirements set out in their respective Member State.

1.3. Target audience

The audience is a wide range of users and stakeholders, including senior technical personnel and procurement decision-makers within hospitals, and healthcare providers such as chief information officers, chief information security officers, chief technology officers, IT teams, procurement officials, general practitioners and IT support staff.

The guidance also addresses medical device manufacturers and suppliers of clinical information and EHR systems, networking solutions, cloud services and related products, helping them understand the cybersecurity requirements expected when delivering solutions to healthcare entities. By doing so, suppliers can better demonstrate compliance and align their offerings with the sector's cybersecurity and policy expectations.

1.4. Policy landscape

The cybersecurity policy landscape relevant to healthcare procurement includes the following.

- **Directive (EU) 2022/2555 (NIS2 Directive)** obliges health entities ([10]) to implement cybersecurity risk management and incident reporting requirements, which directly impact procurement processes.

- **The European Commission communication on the action plan for the cybersecurity of hospitals and healthcare providers (January 2025)** outlines EU-wide initiatives aimed at bolstering cybersecurity in healthcare through four key priorities: prevention, detection, response and deterrence.

- **The Medical Devices Regulation (MDR) and *In Vitro* Diagnostic Medical Devices Regulation (IVDR)** contain cybersecurity requirements ensuring that medical devices and *in vitro* diagnostic medical devices (IVDs) adhere to robust cybersecurity standards throughout their life cycle, from pre-market approval to post-market vigilance.

- **The General Data Protection Regulation (GDPR)** sets requirements for the protection and secure processing of personal health data, significantly influencing procurement requirements regarding data protection and privacy.

- **The European Health Data Space (EHDS) Regulation** aims to standardise secure electronic health data exchange across Member States, facilitating patient empowerment,

([8]) As defined in Article 6(1) of Directive (EU) 2555/2022.
([9]) Any entity providing ICT products, ICT systems or ICT services that a hospital or healthcare provider relies on. When this guidance refers to suppliers, it includes their personnel.
([10]) For the definition of essential and important entities, see Article 3 of the NIS2 Directive.

research and innovation, thus further embedding cybersecurity as a foundational requirement in healthcare procurement.

- **The EU Cyber Resilience Act (CRA)** lays down horizontal cybersecurity requirements for products with digital elements made available on the market. However, products with digital elements to which either the MDR or IVDR apply are not subject to this regulation.

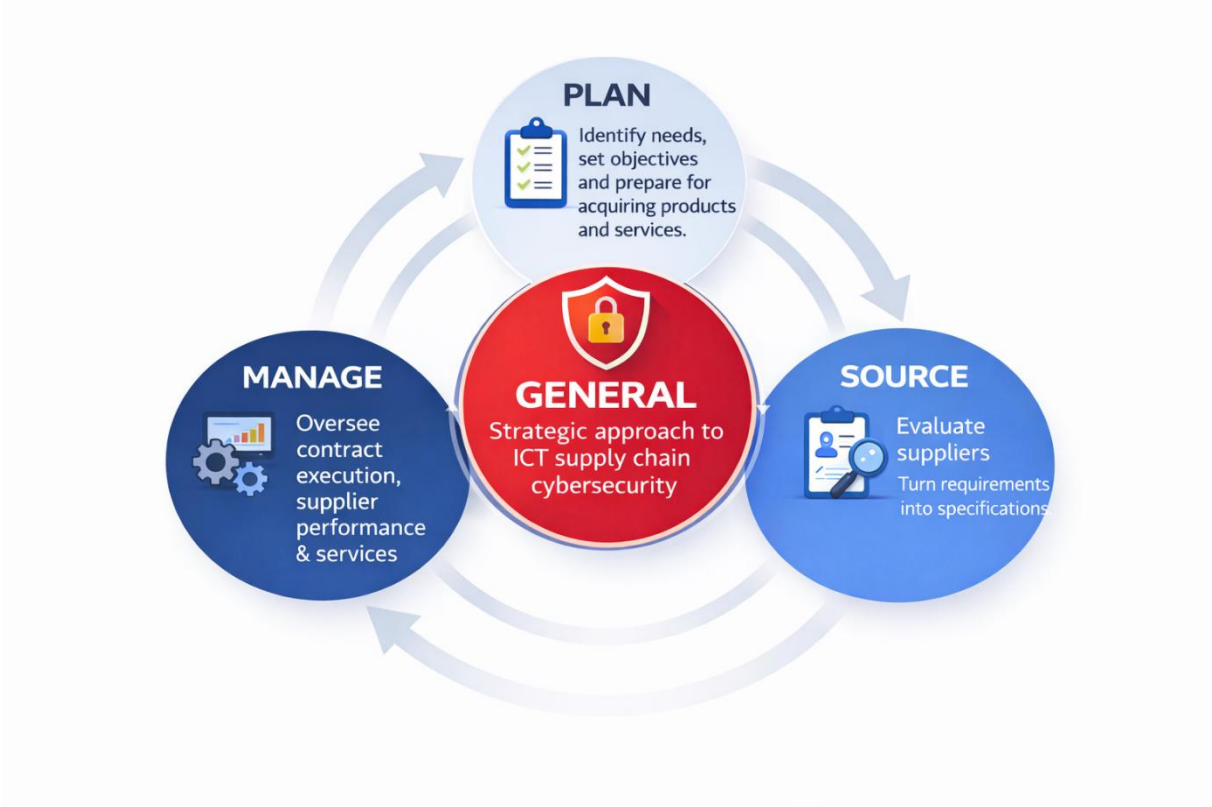
The proposed measures outlined in Section 2.3 are grounded in the requirements and provisions of the aforementioned frameworks, ensuring alignment with current legal and regulatory standards relevant to cybersecurity in the health sector. Any changes or updates to these frameworks may necessitate a review of this document.

2. Procurement life cycle

2.1. Overview

Given the complexity of the healthcare ecosystem – which includes medical devices and IVDs, health information systems, cloud-based and on-premises infrastructure, and operational technologies that support both clinical and administrative functions – cybersecurity must be addressed holistically across the entire healthcare technology infrastructure and its associated services. Also, it is crucial to embed cybersecurity throughout every stage of the procurement life cycle for healthcare-related ICT products ([11]) and services.

The following outlines the key phases of the procurement process and highlights key cybersecurity considerations at each phase.



Before entering the planning phase, hospitals and healthcare providers should first adopt a strategic approach to supply chain cybersecurity risk, formalised through the adoption of a dedicated policy and rooted in a continuous screening of the entire healthcare technology infrastructure and its service dependencies (see Section 2.3.2).

- **Plan phase**. This phase initiates the specific procurement process for the entire healthcare technology infrastructure and its associated services. It encompasses gathering detailed requirements from internal stakeholders, clearly setting objectives and formulating tender

([11]) As defined in Article 6(12) of Directive (EU) 2555/2022.

specifications to facilitate efficient and cost-effective procurement. Critical to this phase are the explicit identification and assessment of cybersecurity risks relevant to the intended procurement, alongside defining precise cybersecurity requirements aligned with standards such as International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 27001, National Institute of Standards and Technology Special Publication (NIST SP) 800-53, or applicable national e-health cybersecurity frameworks. For example, when procuring a cloud-based health data analytics service, the technology lead, in collaboration with the information security lead of the hospital or the healthcare provider and data governance specialists, must incorporate cybersecurity and privacy requirements explicitly into the tender documentation.

- **Source phase**. This phase involves initiating the procurement tender process, evaluating received proposals and selecting suitable ICT system, product or service suppliers. At this stage, previously defined cybersecurity requirements transformed into technical specifications are evaluated in submitted proposals. These include:
    - explicit obligations for minimum acceptable security standards;
    - clearly defined responsibilities for incident management;
    - required disclosure of known vulnerabilities; and
    - obligations for suppliers regarding timely software patching and maintenance.

  When feasible, the evaluation of proposals should be conducted by a multidisciplinary committee – including IT, cybersecurity, clinical engineering and legal/regulatory representatives – to ensure both functional and cybersecurity adequacy.

- **Manage phase**. This phase focuses explicitly on post-procurement oversight, covering the implementation, management and maintenance of the entire healthcare technology infrastructure and its associated services. It ensures that the ICT systems, products and services meet the agreed-upon specifications, are delivered on time and remain within budget, all while effectively managing cybersecurity risks, contractual relationships and regulatory compliance. The hospital or the healthcare provider continuously monitors supplier performance, enforces cybersecurity measures, manages incident responses and collects user feedback to maintain the quality and security of the delivered solutions. There is ongoing monitoring for cybersecurity incidents and emerging threats, along with implementation of corrective actions such as software updates or security configuration changes. Secure end-of-life management is crucial, including proper sanitisation and disposal of systems and devices that may store sensitive health or personal data.

2.2. List of procurement types

The supply chain includes various types of entities:

- ICT supplier (including software and hardware supplier),
- manufacturer,
- managed service provider,
- managed security service provider,
- cloud service supplier, and
- user.

The following procurement types have been identified ([12]):

- clinical information systems (CIS),
- medical devices,
- network equipment,
- remote care systems,
- mobile client devices,
- identification systems,
- healthcare facility infrastructure,
- industrial control systems and supervisory control and data acquisition (ICS/SCADA), including building management systems (BMS),
- professional services.
- cloud services,
- managed service provider services,
- managed security service provider services,
- system integrator services,
- web services,
- artificial intelligence (AI) enabled products and assisted services.

For free and open-source software (OSS), the entities that maintain and distribute software openly may not be considered direct service suppliers. This applies when there is no contractual relationship between the relevant entity and the open-source project beyond adherence to a standardised copyright license, or where the contractual relationship is with an OSS steward (Regulation 2024/2847, Article 3(14) 'provides support on a sustained basis for the development and ensures the viability of those products').

2.2.1. Cross-cutting considerations for AI-enabled products and AI-assisted services[13]

AI-related procurement risks are not limited to products explicitly marketed as AI-enabled. They may also arise where AI functionality is embedded in another product or service, accessed through a third-party AI service or interface, or used by a supplier or subcontractor in software development, technical support, security testing, documentation, data analysis or other activities performed under the contract. Healthcare entities should therefore determine whether and how AI is involved throughout the supply chain, including following contract award and subsequent changes to the service or AI functionality.

Where AI is involved, procurement documentation should require suppliers to disclose the intended purpose and scope of the AI functionality, the AI provider and deployment model, relevant data processing arrangements, categories of data processed, storage and retention arrangements, subprocessors, human oversight measures, logging capabilities and procedures for notifying the healthcare entity of material changes affecting the AI system or its processing activities. Where customer data may be used for the development, training or further improvement of AI models, suppliers should clearly identify the relevant processing purposes and legal basis.

([12]) See Annex A for descriptions.

[13] Procurement, accountability and risk-management principles derived from Regulation (EU) 2024/1689 (AI Act); Regulation (EU) 2016/679 (GDPR), Directive (EU) 2022/2555 (NIS2), EDPB Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models and ENISA guidance on AI cybersecurity and lifecycle risk management.

Sensitive health, personal, security or infrastructure information should not be submitted to external AI services or used for AI model development unless expressly and explicitly authorised following appropriate legal, data protection, cybersecurity and clinical risk assessments. Contracts should also specify data return and deletion obligations at contract termination, including, where applicable, user inputs, AI-generated outputs, logs and other derived data.

2.3. List of measures per procurement phase

Below is a list of cybersecurity measure groups organised by procurement phase. They address the overall procurement process, ranging from general practices and system preparation to specific security requirements tailored to each phase of procurement.

In the following sections, the security measures are presented at the objective level, while detailed implementation guidance is provided in Section 3. The measures under the 'General' category are presented only at the objective level, as they represent horizontal practices that cut across all procurement phases. Due to their broad applicability, references and implementation details for these measures are considered easily accessible. For entities with limited cybersecurity capacity the ENISA guidance on *Cyber Hygiene in the Health Sector* is recommended ([14]).

To improve readability, each measure includes the following components:

a) a code/Identifier – specifies whether the measure is part of the entity's strategic approach to ICT supply chain cybersecurity (e.g., GENERAL-01), or belongs to one of the three procurement phases (e.g., PLAN-02, SOURCE-01) of the measures; and
b) an objective – a brief narrative that explains what should be achieved with the specific measure.

Annex B provides details on the structure of each measure.

2.3.1. General

We consider that every entity should have in place the following general security measures to support the procurement process throughout all its phases (plan, source, manage).

General measures

General measures	
Group	**Objective**
GENERAL-01	Adopt a strategy for the supply chain cybersecurity of the entire healthcare technology infrastructure and its associated services that embeds cybersecurity as a core requirement in all purchasing decisions, ensuring alignment with the applicable legal framework ([15]).
GENERAL-02	Allocate adequate financial and human resources to implement the strategy.

([14]) ENISA, *Cyber Hygiene in the Health Sector*, 2025, https://data.europa.eu/doi/10.2824/3818935.
([15]) This includes formalising a strategic approach to cybersecurity, with management bodies actively approving and overseeing cybersecurity risk-management measures to foster accountability and ensure the resilience of essential and important entities. Management bodies are defined as in the context of Article 20 of the NIS2 Directive. For more details on ICT supply chain cybersecurity good practices see ENISA, *Good Practices for Supply Chain Cybersecurity*, June 2023, https://data.europa.eu/doi/10.2824/805268.

General measures	
GENERAL-03	Create and maintain an up-to-date and detailed directory of all critical suppliers of the entire healthcare technology infrastructure and its associated services, along with information about the products or services they provide and their cybersecurity qualifications.
GENERAL-04	Identify, assess and remediate known vulnerabilities in systems and services, leveraging threat intelligence and collaboration with product/service suppliers of the entire healthcare technology infrastructure and its associated services.
GENERAL-05	Implement a robust patch management process.
GENERAL-06	Design and maintain a secure network architecture with strong access controls to isolate critical ([16]) systems and limit damage from potential breaches.
GENERAL-07	Ensure the continuity of critical operations during and after cyber incidents by establishing detailed procedures for system recovery, emergency response and crisis management.
GENERAL-08	Ensure comprehensive and continuous logging and monitoring capabilities are embedded across all networks and information systems, including those newly acquired.
GENERAL-09	Ensure the confidentiality, integrity and availability of all sensitive health and personal data within the procured solutions.
GENERAL-10	Cultivate a robust cybersecurity culture across the hospital or the healthcare provider by providing regular and targeted awareness training to all internal staff, and by ensuring the demonstrable security competence of all external partners engaged throughout all procurement phases.
GENERAL-11	Evaluate the effectiveness of implemented security measures.

2.3.2. Plan phase

Plan measures

Plan measures	
Group	**Objective**
PLAN-01	Establish a thorough risk identification process in the procurement process.
PLAN-02	Ensure that all new ICT systems, products, and service suppliers comply fully with applicable security, privacy and regulatory requirements.
PLAN-03	Develop and enforce a supply chain cybersecurity policy which covers the entire healthcare technology infrastructure and its associated services.
PLAN-04	Establish cybersecurity requirements within all procurement documentation.

([16]) Based on confidentiality, integrity, authenticity and availability requirements, to indicate the protection required according to their sensitivity, criticality, risk and business value.

Plan measures	
PLAN-05	Incorporate comprehensive cybersecurity clauses into supplier contracts, including requirements governing the use of AI systems by suppliers and subcontractors.
PLAN-06	Include dedicated cloud-specific security and compliance clauses in all procurement documents and contracts for cloud services.
PLAN-07	Ensure cross-functional stakeholder involvement during procurement.

2.3.3. Source phase

Source measures

Source measures	
Group	**Objective**
SOURCE-01	Prioritise the selection of ICT system, product and service suppliers who demonstrate certified compliance with relevant security standards and regulations ([17]).
SOURCE-02	Conduct a thorough data protection impact assessment (DPIA), including AI enabled and AI-assisted processing of sensitive health data.
SOURCE-03	Evaluate and verify the specific technical security requirements of ICT systems, products and services, including AI models, during selection and contract negotiations.
SOURCE-04	Ensure that all equipment and software are procured exclusively through authorised and trusted channels.
SOURCE-05	Require ICT system, product or service suppliers to adopt a secure software development life cycle (SDLC) approach that ensures healthcare systems, including machine learning practices are designed and maintained with security by design.
SOURCE-06	Require suppliers to maintain transparency and accountability regarding third-party software and firmware components, including AI-related components used in their IT and operational technology environments.

([17]) Devices certified under the Medical Device Directive (93/42/EEC) and the Active Implantable Medical Devices Directive (90/385/EEC) can benefit from the transition of these directives to the MDR and IVDR.

2.3.4. Manage phase

Manage measures

Manage measures	
Group	**Objective**
MANAGE-01	Ensure that suppliers are contractually obligated to manage and remediate vulnerabilities throughout the life cycle of their products.
MANAGE-02	Maintain an accurate and up-to-date inventory of the entire healthcare technology infrastructure including AI functionality and models.
MANAGE-03	Ensure that suppliers notify the organisation of any cybersecurity incidents related to their products or services.
MANAGE-04	Embed continuous improvement in cybersecurity risk management processes.
MANAGE-05	Implement secure decommissioning and exit procedures for assets, services and AI related components that prevent data breaches and unauthorised access to sensitive information during disposal or retirement.

3. Implementation guidance

Each cybersecurity measure is described using a structured format which communicates its relevance and priority across different types of healthcare providers. The structure includes the following components:

- code/identifier – specifies whether the measure belongs to one of the three procurement phases (e.g., PLAN-02, SOURCE-01);
- title (e.g., identify risks in procurement, legal and compliance requirements);
- objective – explains what should be achieved with the specific measure;
- implementing guidance – a detailed list of practical steps, responsibilities or best practices that support the measure's implementation;
- related procurement type – indicates which types of procurement, one or more from the list in Section 2.2, the cybersecurity measure applies to:
    - recommended – identifying the types of procurement for which the measure is considered necessary,
    - nice-to-have – identifying the types of procurement for which the measure is desirable.

'Recommended' measures are essential cyber hygiene practices such as using strong passwords, enabling MFA, keeping software updated, installing an antivirus and implementing regular data backups based on the type and scope of each supplied service or product. 'Nice-to-have' measures, on the other hand, offer enhanced security layers and go beyond basic protection. The distinction depends on the organisation's risk tolerance, resources and industry, with recommended measures for essential protection and nice-to-have items for superior defence.

Plan measures

PLAN-01	Identify risks in procurement

Objective

To establish a thorough risk identification process in the procurement of critical systems, products and services by assessing potential cybersecurity threats and evaluating how new acquisitions may alter the organisation's overall risk profile ([18]).

Implementing guidance

- Use risk assessment results: leverage results from existing risk assessments to evaluate whether additional cybersecurity controls, risk mitigations or budget reallocations are necessary for the proposed procurement. This evaluation should determine whether the acquisition aligns with the hospital's or health provider's established risk tolerance and overall risk posture. If risks introduced by the new system, product or service exceed acceptable thresholds, the entity should reassess procurement feasibility or consider alternative solutions.
- Interoperability and legacy risks: plan for how the new solution will interact with existing systems and mitigate any legacy technology issues. Legacy technologies might use outdated protocols or unsupported software. Identify whether the new system needs to interface with such technologies, and if so, include requirements for secure integration. This may involve using middleware or gateways to bridge old and new systems securely.

Related procurement types **Recommended:** all procurement types.

PLAN-02	Legal and compliance requirements

Objective

To ensure that all system, product and service suppliers comply fully with applicable security, privacy and regulatory requirements ([19]) prior to procurement. This includes verifying adherence to mandated standards, certifications and regulations such as ISO 27001, the EHDS Regulation and the MDR/IVDR to maintain legal compliance and safeguard sensitive health information.

([18]) This includes, where relevant, incorporating findings from coordinated security risk assessments as required by Article 21(3) of Directive (EU) 2022/2555, ensuring informed decision-making that minimises exposure to new or amplified risks.

([19]) Including healthcare data protection laws (e.g., GDPR), national cybersecurity regulations and internal policies.

Implementing guidance

- Develop a compliance checklist that incorporates key cybersecurity requirements stemming from key pieces of cybersecurity legislation.
- Engage legal experts to validate compliance mappings, ensuring accuracy.
- Include contractual clauses that assign responsibility to suppliers for meeting defined compliance, cybersecurity and risk-management requirements.

Related procurement types	**Recommended:** medical devices / IVDs, CIS, remote care systems. **Nice-to-have:** cloud services, AI-enabled products, professional services.

PLAN-03	Supply chain security policy

Objective

To develop and enforce a supply chain cybersecurity policy that guides procurement activities, mitigates risks from third-party vulnerabilities and ensures the protection of the entire healthcare technology infrastructure and its associated services. The policy must clearly define roles and responsibilities for all stakeholders involved, fostering accountability and a coordinated approach to supply chain security.

Implementing guidance

Supplier criteria: set minimum cybersecurity criteria that prospective system, product or service suppliers must meet to be eligible. Those criteria shall include the following:

- the cybersecurity practices of the suppliers, including their secure development procedures;
- the ability of the suppliers to meet cybersecurity specifications set by the relevant entities;
- the overall quality and resilience of systems, products and services and the cybersecurity risk-management measures embedded in them, including the risks and classification level of the systems, products and services; and
- the ability of the relevant entities to diversify sources of supply and limit ICT system, product or service suppliers lock-in, where applicable.

Supply chain security for open-source components: the ICT system, product or service suppliers commit to keeping not just the licences required for software, but also its libraries and dependencies, up to date with patches. If possible, it would be best if bidders can provide a listing of the open-source components in the system and require adherence to relevant EU regulations like the CRA for security and documentation.

Related procurement types	**Recommended:** CIS, medical devices / IVDs, remote care systems, network equipment, AI-enabled products, ICS/SCADA, healthcare facility infrastructure. **Nice-to-have:** all other procurement types.

PLAN-04	Requirement's definition

Objective

To establish clear, detailed and enforceable cybersecurity requirements within all procurement documentation – such as requests for proposals, quotations and technical specifications – that align with applicable standards and regulatory frameworks, ensuring that acquired products and services meet the organisation's security expectations.

Implementing guidance

- Enumerate specific security features and controls that the product or service **must** have. For example, require support for encryption of data in transit and at rest, robust user access controls (role-based access and MFA), audit logging capabilities and secure configuration options out of the box.
- Include life cycle requirements: the system, product or service suppliers should provide security updates for the expected lifespan of the product and have a plan for end-of-life (e.g., device replacement or extended support).
- Set expectations for how the system, product or service suppliers will assist with incident response (for instance, requiring a point of contact for security incidents and a maximum response time). Incident reporting obligations can be built into requirements, for example, the RFP can state that the system, product or service suppliers must agree to notify the buyer within 24 hours of any breach affecting the product or service.
- Consider open-source certifications as evidence: where applicable, use ICT system, product or service suppliers' certifications as a tiebreaker or quality indicator in your evaluation plan. Some OSS projects have official partner certification programmes (for example, Nextcloud or Univention certify service partners), which can prove a bidder's close collaboration with the product's maintainers.
- Check open-source sustainability requirements: check explicit quality and sustainability requirements in the tender. For example, weight factors such as ICT system, product or service suppliers' expertise, support arrangements, security practices and community contributions alongside cost. This ensures you identify a proposal that is economically advantageous in the long run, not just the cheapest on paper. Ask for evidence of the support/partnership with the software vendor or active participation in the community (such as contribution history or employing core maintainers).

Related procurement types	**Recommended:** all procurement types.

PLAN-05	Contractual security clauses

Objective

To incorporate comprehensive cybersecurity clauses into supplier contracts that legally enforce strong security obligations throughout the engagement, in accordance with NIS2 Directive requirements. These clauses must clearly define supplier liability for security breaches or negligence, mandate cyber insurance coverage or indemnification provisions and establish accountability to protect healthcare entities from cyber risks associated with third-party products and services.

Implementing guidance

- Clearly specify the supplier's ongoing security obligations – for example, they must apply security patches promptly and notify the healthcare entity of any vulnerabilities or incidents without undue delay. Include an incident notification clause that obligates the system, product or service suppliers to notify the procuring entity of any security incident affecting the product or any customer data immediately.
- Other terms might include: obligations for the system, product or service suppliers to address and remediate vulnerabilities in their products that pose risks to the customer (with defined timelines for critical fixes), restrictions on subcontracting (the system, product or service suppliers must seek approval for any subcontractors and flow down security requirements to them) and clear provisions for end-of-contract transitions (secure return or destruction of data, continuity of support for a period, etc.).
- Where AI systems are used by suppliers and subcontractors, the contract should define permitted and prohibited uses of AI and require prior disclosure of relevant AI models, providers, hosting arrangements, subprocessors and data flows, while prohibiting the submission of sensitive health, personal, security or infrastructure information to external AI systems without explicit authorisation.
- Include an upstream contribution clause for OSS in your requirements and contracts, ensuring, where feasible and appropriate, that any custom code or patches developed for you will be submitted upstream to the main open-source codebase and released under a recognised open-source license ([20]). Specify how and where this code should be delivered (e.g., the official project repository or a platform like openCode). This ensures the broader community can review and integrate the changes, improving software quality and security for everyone.

Related procurement types	**Recommended:** all procurement types.

([20]) If upstream contribution is not possible, the supplier or the service provider must document the reasons.

PLAN-06	Dedicated cloud procurement clauses

Objective

To include dedicated cloud-specific security and compliance clauses in all procurement documents and contracts for cloud services – such as cloud-based EHR platforms, data analytics and telemedicine – to address the unique risks and regulatory obligations associated with cloud computing in healthcare, ensuring protection of sensitive health data and compliance with applicable laws and standards.

Implementing guidance

- Personal health data must be stored and processed in specified jurisdictions (for example, within the EU or within the country) to comply with data sovereignty laws and facilitate oversight.
- Require the cloud service supplier to detail their redundancy and disaster recovery measures – for instance, the use of multiple geographically separate data centres (availability zones) for high availability, regular backups and an ability to fail over with minimal downtime.
- The contract also obliges the supplier to meet healthcare-specific standards, such as being certified under schemes for cloud security or complying with national guidelines for cloud usage in the health sector.
- The cloud service supplier agrees to promptly inform the healthcare organisation of any incidents (breaches or outages) that could affect them, aligning with the NIS2 Directive's incident reporting requirements.
- Ensure the contract states that the healthcare tenant will have control over data access and encryption keys where possible, and that the supplier will implement strong isolation between different customers.

Related procurement types **Recommended:** cloud services.

PLAN-07	Engagement of all relevant internal actors

Objective

To foster active stakeholder engagement across management, IT, clinical and legal teams throughout the procurement process, ensuring informed decision-making, compliance with the NIS2 Directive and alignment with healthcare operational goals. This collaborative approach

promotes shared responsibility for cybersecurity risk management, supports uninterrupted patient care and strengthens organisational resilience through effective governance and cyber hygiene practices.

Implementing guidance

- Establish a cross-functional procurement-specific committee with IT, clinical and legal representatives to ensure all perspectives are considered.
- Set specific cybersecurity goals (like secure interoperability or detailed logging) and make sure these goals help fulfil your legal and operational obligations under the NIS2 Directive.
- Conduct workshops to align stakeholders on NIS2 Directive requirements, enhancing awareness and collaboration.
- Document stakeholder inputs to ensure transparency and support compliance audits, facilitating traceability.

Related procurement types **Recommended:** all procurement types.

Source measures

SOURCE-01	System, product or service providers selection

Objective

When feasible, healthcare providers must prioritise the selection of ICT product and service suppliers who demonstrate certified compliance with relevant security standards and regulations, including MDR/IVDR requirements and the EHDS Regulation ([21]). The evaluation process shall comprehensively assess suppliers' cybersecurity posture beyond product features, incorporating third-party audit reviews, development practices and risk assessments of their governance and incident response ([22]) capabilities, thereby ensuring robust security throughout the supply chain.

([21]) Devices certified under the Medical Device Directive (93/42/EEC) and the Active Implantable Medical Devices Directive (90/385/EEC) can benefit from the transition of these directives to the MDR and IVDR.

([22]) 'Incident' refers to the NIS2 Directive definition related to cybersecurity events. This is distinct from 'serious incidents' under the MDR/IVDR, which involve medical device safety and have separate vigilance reporting requirements.

Implementing guidance

- Evaluate incident response plans: assess ICT system, product or service suppliers' plans for incident detection, containment and reporting, ensuring alignment with the NIS2 Directive's 24-hour early warning and 72-hour detailed reporting deadlines.
- Check supply chain oversight: verify that ICT system, product or service suppliers have policies to manage their subcontractors' cybersecurity risks, as required by the NIS2 Directive.
- Conduct background checks: when feasible, organisations should investigate ICT system, product or service suppliers' history of cybersecurity incidents or breaches to assess reliability, in line with the NIS2 Directive's risk-based approach.

Related procurement types	**Recommended:** CIS, medical devices / IVDs, remote care systems. **Nice-to-have:** cloud services, network equipment, managed services, managed security services.

SOURCE-02	DPIA

Objective

To conduct a thorough DPIA in collaboration with the data protection officer whenever a new system processes sensitive personal health data and is likely to result in a high risk to individuals. The DPIA must identify privacy risks, including risks relevant to AI assisted or AI enabled processing – such as cross-border data transfers or use of AI analytics impacting individual rights – and must recommend appropriate measures to mitigate these risks, ensuring compliance with data protection regulations and safeguarding patient privacy.

Implementing guidance

- Incorporate the findings into the procurement requirements: if the DPIA flags high risks (for example, the service would store highly sensitive data externally), you might require the system, product or service suppliers to implement specific safeguards in addition to those given in the tender specification or agree to particular contract terms (like data encryption, access restrictions or enhanced access logging) before proceeding.
- Map AI-related data flows, inputs, prompts, uploaded files, outputs, and any other data processed by AI functionality. Identify access to the data, storage, retention period and whether they are used for model training or other secondary purposes.
- Check that manufacturers and suppliers have clear processes to evaluate potential impact on patients across their products and services, checking both broadly (all related products or services offered) and deeply (specific components within each product or service).

Related procurement types	**Recommended:** AI-enabled products, CIS, identification systems, medical devices / IVDs, remote care systems. **Nice-to-have:** mobile client devices, web services, cloud services.

SOURCE-03	Technical requirements

Objective

To thoroughly evaluate and verify the specific technical security requirements of system, products and service suppliers during selection and contract negotiations, ensuring that all technical conditions meet organisational security standards and regulatory obligations before finalising procurement decisions.

Implementing guidance

- **Access control:** in many cases remote access is necessary to maintain systems or products (e.g., for troubleshooting medical equipment). During procurement, insist on strict controls for any remote access. The contract or service agreement should state that remote access must be pre-approved and take place only within agreed time windows. Also require that system, product or service suppliers' personnel can only access the specific device or module they support – not the wider healthcare entity's network. Regularly authenticate and authorise external connections, utilise MFA for privileged users, ensure updates require secure authorisation, strengthen passwords by avoiding defaults or hardcoded credentials and implement anti-replay protections for critical communications.
- **Maintenance:** all maintenance and update activities must occur over secure, encrypted channels (e.g., VPN with MFA, or other encrypted tunnels) and are digitally signed and verified, to protect data in transit.
- **Network:** system, product or service suppliers must use secure methods (VPN with MFA, one-time access tokens, etc.), strong cryptographic authentication for personnel, communications, updates, and encrypted external connections across all healthcare services and devices, considering hardware-based solutions when feasible.
- **High-quality support:** check that clear requirements for ongoing support and maintenance are in place. Also, validate that the potential contractor explains how they will handle support (deep code-level fixes) for the components. The contract should stipulate guaranteed response times (SLAs) for critical issues and suppliers of the ICT systems, products or services must demonstrate their capability to meet these requirements. Ensure that suppliers of systems, products or services have submitted evidence demonstrating how they will meet the required SLAs for critical issues.

- **Security documentation:** suppliers of the systems, products or services must provide security documentation as part of procurement. Healthcare suppliers should prioritise certified products.

Related procurement types	**Recommended:** medical devices / IVDs, remote care systems, EHR. **Nice-to-have:** managed services, CIS, network equipment, ICS/SCADA, healthcare facility infrastructure.

SOURCE-04	Requirements for supply chain security

Objective

To ensure that all equipment and software are procured exclusively through authorised and trusted channels, incorporating measures that guarantee product integrity and authenticity. This approach aims to minimise risks associated with counterfeit or compromised components by avoiding grey-market and unauthorised third-party resellers, thereby protecting the healthcare environment from supply chain threats.

Implementing guidance

- Add clauses into the procurement specifications stipulating that hardware devices should be original and sourced from the official manufacturer or certified distributors.
- For software, mandate that system, product or service suppliers provide checksums or digital signatures for installation packages and verify these before deployment to ensure no tampering occurs during transit.
- For critical equipment, healthcare entities can also leverage technologies like device identity certificates or software code signing as acceptance criteria. For example, a network device might be required to support an integrity check on first boot to prove its firmware is factory-original.

Related procurement types	**Recommended:** medical devices / IVDs, network equipment. **Nice-to-have:** CIS, ICS/SCADA, healthcare facility infrastructure.

SOURCE-05	SDLC

Objective

To require system, product or service suppliers to adopt an SDLC approach that ensures healthcare systems are designed and maintained with security by design. Where AI is involved, the service development approach should extend to machine learning life cycle. This includes implementing hardware-based security measures where feasible, cryptographically authenticating software updates and verifying software authenticity prior to deployment to protect system integrity.

Implementing guidance

- System, product or service suppliers and suppliers placing their devices on the market or putting them into service must ensure that products and their respective components are designed and manufactured in accordance with the applicable legal requirements (CRA, MDR, IVDR and EHDS Regulation).
- Also, suppliers should restrict debug access and apply physical tamper protections on devices.
- For software, verify data integrity cryptographically, validate external data rigorously and safeguard essential configuration data. Also, suppliers should opt for secure code execution with industry-standard intrusion detection measures and thorough automated and manual code reviews.
- Where AI functionality is used, require suppliers to document and protect the machine learning life cycle and material changes should undergo security testing and approval.
- Updates and security: during evaluation, review how each ICT system, product or service suppliers' plans to handle updates and security throughout the duration of the contract. Look for a clear plan in each proposal on how the ICT system, product or service suppliers will upstream any modifications. The proposal acknowledges the need to track and patch vulnerabilities in the OSS components (e.g., prompt updates when security fixes are released by the community). Favour ICT system, product or service suppliers who explicitly commit to contributing their changes back to the core OSS project and have processes in place to do so (e.g., following the project's contribution guidelines, engaging with maintainers).

Related procurement types	**Recommended:** medical devices / IVDs, web services, mobile client devices, remote care systems. **Nice-to-have:** CIS, AI-enabled products, cloud services, identification systems.

SOURCE-06	Supply chain cybersecurity transparency

Objective

To enhance supply chain cybersecurity by requiring suppliers, especially large companies and pharmaceutical suppliers, to maintain transparency and accountability regarding third-party software and firmware components used in their IT and operational technology environments. This includes AI related components and dependencies. This transparency is critical to identifying and mitigating supply chain risks effectively.

Implementing guidance

Vulnerability disclosure: Contractually obligating an ICT system, product or service supplier to notify the procuring entity of any security issues in their products and deliver patches promptly enforces timely risk mitigation. While pharmaceutical products are chemical, this requirement also applies to the pharmaceutical industry's digital suppliers under frameworks like the NIS2 Directive. In practice, implementation may involve enhancing the supplier evaluation process to include security posture assessments and clearly specifying in contracts that failure to remediate known vulnerabilities within a reasonable time frame constitutes a breach of agreement.

Related procurement types	**Recommended:** CIS, medical devices / IVDs, remote care systems. **Nice-to-have:** ICS/SCADA, healthcare facility infrastructure.

Manage measures

MANAGE-01	Vulnerability disclosure and patch management obligations

Objective

To ensure that suppliers are contractually obligated to manage and remediate vulnerabilities throughout the life cycle of their products by maintaining a formal process for receiving vulnerability reports from healthcare organisations, researchers, and users; promptly analysing root causes; and developing and deploying patches or mitigations without undue delay to maintain system security and integrity ([23]).

Implementing guidance

- Regularly check system, product or service suppliers for any patches or security bulletins related to your deployed products.

([23]) Medical device suppliers should also adhere to the MDR/IVDR and relevant obligations for a post-market surveillance system.

- If a critical vulnerability is found in their product (whether by your team or externally), the system, product or service suppliers must treat it with urgency and provide a software update or compensating control in a defined time frame.
- Entities integrate supplier patch management into their own change management and risk management procedures.
- Require the supplier to regularly provide evidence of patching and updating activities for the supplied system or product, including but not limited to patch logs, reports, and change management records.
- Monitor and patch security vulnerabilities of OSS: stay vigilant about security updates for all OSS components in your solution. Establish a routine (or require the ICT system, product or service suppliers) to monitor security advisories from the OSS communities and to apply patches or upgrades in a timely fashion when vulnerabilities are disclosed.

Related procurement types	**Recommended:** medical devices / IVDs, CIS. **Nice-to-have:** remote care systems, cloud services, network equipment, ICS/SCADA, healthcare facility infrastructure.

MANAGE-02	Maintenance

Objective

To maintain an accurate and up-to-date inventory of all IT assets and their configurations managed by the healthcare provider – including newly procured systems – and to document configuration baselines such as secure settings and network parameters. This ensures ongoing visibility and control over system security postures throughout their life cycle.

Implementing guidance

- If maintenance is performed by suppliers or third parties, they must commit to performing periodic and timely maintenance on the entity's assets and using effective mechanisms and tools.
- Where AI functionality is involved, also record its intended purpose, model and service provider, relevant APIs, categories of data processed, subprocessors, human oversight and fallback arrangements.
- For ongoing maintenance, if the supplier or a third party performs maintenance tasks (software updates, hardware part replacements, calibration of devices, etc.), they must commit to doing so in a timely and secure manner. This includes using only authorised tools, following agreed procedures (as per the technical requirements mentioned in this document) and providing maintenance reports.

- Upstreaming and open licensing: where feasible and appropriate, actively ensure the ICT system, product or service suppliers fulfil the obligation to contribute code upstream and publish improvements. All patches, new features or localisation work performed for your system should be submitted to the official project or otherwise made publicly available as agreed ([24]).
- Independence for OSS from ICT system, product or service suppliers: for critical systems, preserve your autonomy over the open-source solution. Require comprehensive documentation and ideally have your technical staff shadow or participate in the implementation process to gain first-hand experience. If the ICT system, product or service suppliers go out of business or the contract ends, entities must have sufficient documentation and access to the open-source community to obtain support or engage an alternative supplier.

Related procurement types	**Recommended:** managed services. **Nice-to-have:** medical devices / IVDs, network equipment, ICS/SCADA, remote care systems, healthcare facility infrastructure.

MANAGE-03	Incident monitoring

Objective

To establish processes that ensure suppliers promptly notify the hospital or healthcare provider of any cybersecurity incidents involving their products or services and actively collaborate in incident response efforts to enable timely mitigation and minimise operational impact.

Implementing guidance

- The supplier must notify the healthcare entity without undue delay of incidents that could impact the security of the entity's network and information systems. Suppliers know whom to contact in an entity organisation (e.g., the information security lead or incident response team) and understand what qualifies as an incident (for example, a breach of their cloud environment hosting your data, a discovered intrusion or malware in their product).
- Set up a simple reporting mechanism – this could be as straightforward as an email or phone hotline to your security team, or access to a portal for incident reporting. Internally, treat supplier-reported incidents with the same seriousness as internal ones: log them, assess impact, and respond or mitigate as needed.

Related procurement types	**Recommended:** managed services, CIS, cloud services, medical devices, remote care systems.

([24]) If upstream contribution is not possible, the supplier or the service provider must document the reasons.

	Nice-to-have: managed security services.

MANAGE-04	Continuous improvement

Objective

To embed continuous improvement in cybersecurity risk management processes, enabling healthcare entities to adapt proactively to emerging threats and to enhance defences through innovative technologies like AI-based threat detection. This approach ensures sustained resilience and the ongoing effectiveness of security measures in a dynamic threat landscape, in compliance with NIS2 Directive requirements.

Implementing guidance

- Stay informed on threat landscapes: subscribe to threat intelligence feeds and participate in information-sharing platforms.
- Conduct regular risk assessments: update risk assessments at least annually to reflect new threats and vulnerabilities, as per the NIS2 Directive.
- Implement feedback loops: use incident data and lessons learned to refine security measures, aligning with NIS2 Directive's continuous improvement focus.
- Adopt new technologies: evaluate and integrate new cybersecurity tools, such as advanced endpoint protection, as they become available.

Related procurement types	**Recommended:** all procurement types.

MANAGE-05	Secure decommissioning/disposal

Objective

To implement secure procedures that prevent data breaches and unauthorised access to sensitive information during the disposal or decommissioning of IT assets. This ensures the protection of patient data, maintains data integrity and supports compliance with data protection regulations such as the GDPR, thereby complementing the security objectives of the NIS2 Directive.

Implementing guidance

- Establish disposal policies: define procedures for erasing data and recycling or destroying hardware, ensuring no residual data remains.
- Use secure erasure tools: employ software meeting standards like NIST 800-88 for data sanitisation to ensure complete data removal.
- Track asset life cycles: maintain an inventory of IT assets to ensure timely decommissioning, supporting the NIS2 Directive's asset management requirements.
- Comply with data protection law: ensure disposal methods align with the GDPR and other relevant regulations.
- Where AI is involved, verification should also cover prompts, uploaded files, outputs, embeddings, fine-tuning datasets and other derived data, including data retained and deletion confirmations.
- ICT system, product or service suppliers' independence for OSS: for critical systems, preserve your autonomy over the open-source solution. Insist on comprehensive documentation and ideally have your technical staff shadow or participate in the implementation. If the ICT system, product or service suppliers go out of business or the contract ends, you should have sufficient documentation and access to the community to seek help or bring in an alternative supplier.

Related procurement types	**Recommended:** CIS, medical devices / IVDs, remote care systems. **Nice-to-have:** network equipment, identification systems.

4. Use case / scenarios

To demonstrate the practical applicability of the aforementioned security measures, we have developed two fictitious scenarios reflecting common challenges within the daily operations of the healthcare ecosystem: (a) the procurement of medical equipment by a large hospital; and (b) the procurement of cloud-based digital services.

These scenarios were chosen because they represent high-risk and high-impact processes that are frequently encountered in hospitals and healthcare providers. Both involve complex stakeholder interactions, sensitive data flows and stringent regulatory requirements – making them ideal test cases for evaluating the effectiveness, robustness and adaptability of the proposed security measures in real-world contexts.

To facilitate ease of reference and practical implementation, we have codified an extensive set of security measures into a structured and accessible format. Each measure is considered to contribute to one or more of the objectives described in Section 2.3. To group them, each measure has been assigned a unique identifier and is organised systematically in the checklist provided in Annex B. For example, the measure GENERAL-03.08 refers to the eighth measure of the objective GENERAL-03 (‘Up-to-date and detailed directory of all critical suppliers’); PLAN-02.01 refers to the first measure of the objective PLAN-02 (‘New ICT systems, products, and service suppliers comply fully with applicable security, privacy, and regulatory requirements.’)

This codification not only enhances clarity and traceability but also supports consistent application across various scenarios, including risk assessments, procurement processes and compliance audits.

4.1. Use case / Scenario 1: Procurement of radiology equipment in a large hospital

The procurement of medical devices in hospitals and healthcare providers requires a proactive cybersecurity strategy that spans the plan, source and manage phases of the procurement process. By implementing measures such as risk assessments, due diligence, security specifications, patch management and staff training, hospitals and healthcare providers can procure products, systems or services that take cybersecurity into account. This not only ensures compliance with the NIS2 Directive but also safeguards patient care, maintains operational continuity and protects against reputational and legal consequences.

4.1.1. Background

AABB hospital is one of the largest public healthcare facilities in Northern Europe and delivers advanced medical treatments to thousands of patients annually. The hospital depends on a sophisticated network of medical devices/IVDs, including diagnostic tools, patient monitoring systems and therapeutic equipment, many of which are integrated into its EHR system for real-time data sharing. These interconnected devices are critical to patient care but also present potential cybersecurity risks due to their network connectivity.

AABB hospital is procuring a new fleet of networked radiology machines from a global manufacturer. These machines perform advanced imaging techniques, such as CT scans and MRIs, and are connected to its internal network and EHR systems for seamless data sharing and analysis.

Depending on its size and according to the national legislation, every hospital can be classified as either an essential or important entity, requiring them to implement stringent legally binding cybersecurity measures. In order to comply with national law which transposes the NIS2 Directive, the hospital is reviewing its procurement processes. Recognising the rising threat of cyberattacks targeting healthcare, AABB Hospital aims to integrate cybersecurity measures into every phase of the procurement cycle for medical devices/IVDs.

To this end, the hospital has conducted a scenario analysis for procuring new medical devices such as these radiology machines, to identify cybersecurity risks associated with procuring medical devices and to determine the necessary steps to mitigate these risks while ensuring compliance with the NIS2 Directive. In this use case / scenario the type of procurement is 'Medical devices'.

4.1.2. Good practices for procurement

Staff involved in the procurement process should use the checklist in Annex B to identify the measures relevant to the procurement of medical devices/IVDs across the plan, source and manage phases. This applies to all phases of the procurement process (plan, source and manage).

The measures below are an illustrative extract from the checklist in Annex B, selected for this scenario:

General measures

General measures	
Group	**Objective**
GENERAL-03.08	Ensure that suppliers of medical equipment are evaluated for security posture as part of the supplier management programme.
GENERAL-04.04	Verify that a basic unique device identifier – device identifier (UDI-DI) ([25]) has been assigned to the device and is correctly documented, the intended purpose of the device is clearly defined, and a comprehensive description of the device, including variants and accessories, is available.
GENERAL-05.01	Ensure that the patch management policy covers all critical systems and equipment and that security patches from ICT system, product or service suppliers are applied promptly according to schedule.
GENERAL-05.02	Verify that patching procedures include testing patches on non-production device samples and that any devices which cannot be patched have documented compensating controls.
GENERAL-06.02	Confirm that medical device networks are isolated or on dedicated segments, preventing unauthorised access via general networks.
GENERAL-06.08	Verify that remote maintenance access to medical devices is strictly controlled (e.g., via virtual private network (VPN) with multifactor authentication (MFA)) and logged. One-time and time-limited sessions should be used, without the use of permanent accounts, as a condition for the

([25]) In IT security, especially in healthcare, IoT or industrial systems, UDI-DI refers to the device identifier portion of a unique device identifier, especially in regulated fields like healthcare. It's used for identifying and managing hardware assets, ensuring compliance and improving security posture in environments where device integrity and traceability are critical.

General measures	
	procurement, with the possibility of refusing the offer in case of non-compliance. If remote access is not used regularly, it should be disabled and enabled only when necessary, and traffic should be encrypted.
GENERAL-07.02	Ensure continuity plans address availability of medical devices during outages (e.g., backup devices or manual alternatives).
GENERAL-07.05	Check that device failover tests (e.g., backup procedures) are documented and result in updates to continuity planning.
GENERAL-08.05	Check that event logs from medical devices are collected (if possible) and stored securely for later analysis.

Plan measures

Plan measures	
Group	**Objective**
PLAN-02.01	Ensure procurement documentation lists security and regulatory requirements (e.g., MDR, Health Insurance Portability and Accountability Act, GDPR) relevant to medical devices. Best practice is to request the medical device security disclosure (MDS2) ([26]) form from the device supplier during procurement.
PLAN-02.02	Check that ICT system, product or service supplier's bids for medical devices include evidence of following accepted cybersecurity guidelines, regulations (e.g., MDR) and standards or relevant certifications (e.g., ISO 27001, IEC 62304).
PLAN-02.05	Ensure legal review validates that contracts include data protection clauses and breach notification obligations for device suppliers.

Source measures

Source measures	
Group	**Objective**
SOURCE-01.01	Check that ICT system, product or service supplier selection criteria prioritise suppliers with certified or independently assessed security postures.
SOURCE-01.02	Verify that evaluations of ICT system, product or service supplier bids include assessment of the supplier's cybersecurity practices and history of security incidents.

([26]) The MDS2 form is a standardised document used by medical device manufacturers to communicate the cybersecurity features and security-related information of their devices to healthcare delivery organisations, such as hospitals and clinics. The MDS2 provides a standardised security profile for the device and aids in risk assessment.

Source measures	
SOURCE-01.07	Confirm that for critical procurements, a supplier risk assessment is performed examining the ICT system, product or service supplier's cyber incident history and overall security governance.
SOURCE-01.08	Ensure that ICT system, product or service supplier's incident response plans are assessed for alignment with NIS2 Directive timelines (24-hour early warning, 72-hour notification) during selection.
SOURCE-01.10	Ensure that any critical ([27]) device is correctly classified according to MDR Annex VIII rules, with justification provided.
SOURCE-03.01	Ensure procurement requires strict access controls for ICT system, product or service supplier maintenance (pre-approved, scoped access with MFA).
SOURCE-03.03	Verify that all ICT system, product or service supplier maintenance and updates on devices or software are performed over secure, encrypted channels (e.g., VPN with MFA) and signed digital delivery.
SOURCE-04.01	Ensure procurement specifies that hardware must be obtained directly from authorised manufacturers or certified distributors to guarantee authenticity.
SOURCE-04.02	For medical device software, ensure that software validation has been performed following IEC 62304.
SOURCE-04.04	Check that suppliers provide digital signatures or device certificates for critical equipment ([28]) (e.g., first-boot firmware integrity).
SOURCE-05.01	Verify that suppliers of procured systems follow secure development practices (e.g., devices designed per MDR with hardware security features).
SOURCE-06.01	Check that ICT system, product or service supplier contracts include clauses for timely vulnerability disclosure and patching.

Manage measures

Manage measures	
Group	**Objective**
MANAGE-01.01	Verify that supplier contracts enforce the ICT system, product or service supplier's responsibility to receive vulnerability reports and provide fixes without undue delay.
MANAGE-01.02	Check that a process exists to regularly monitor suppliers' security advisories and security bulletins related to deployed products.
MANAGE-02.04	Confirm that maintenance tasks on medical devices (updates, part replacements) are documented and performed using secure procedures.

([27]) According to Article 51(1) of the MDR, devices shall be divided into classes I, IIa, IIb and III, taking into account the intended purpose of the devices and their inherent risks. Classification shall be carried out in accordance with Annex VIII.
([28]) In line with the entity's risk assessment.

Manage measures	
MANAGE-03.04	Ensure there is an established reporting mechanism (e.g., email, hotline) for ICT system, product or service suppliers to inform the hospital or the healthcare provider of security incidents.
MANAGE-05.03	Ensure that patient data on decommissioned medical devices is sanitised using certified tools and that devices are tracked to prevent unauthorised reuse.
MANAGE-05.04	Confirm that disposal of medical device hardware follows defined procedures and that asset records are updated when devices are destroyed or recycled.

4.2. Use case / Scenario 2: Procurement of cloud services from a private medical centre

Measures such as risk assessments, due diligence, security specifications, monitoring and training can help healthcare entities to securely procure cloud services. This ensures compliance with the NIS2 Directive, safeguards patient privacy and maintains trust, while avoiding reputational, legal and financial consequences.

4.2.1. Background

XYZ medical centre provides a broad range of medical services to a diverse patient base in a country in central Europe, from primary care services to x-rays and biochemical testing. The centre relies on digital tools to manage patient records, schedule appointments and deliver telemedicine consultations. To enhance efficiency and accessibility, XYZ is considering procuring a cloud-based system to host its EHR service to store and process sensitive patient data, including medical histories, prescriptions and billing information.

As a healthcare provider, XYZ falls under the scope of the NIS2 Directive. Depending on its size and according to the national legislation, XYZ might be classified as either an essential or important entity, requiring them to implement stringent cybersecurity measures, including supply chain security for procured services like cloud-based systems.

Recent cyberattacks targeting healthcare providers have exploited vulnerabilities in cloud services, prompting XYZ medical centre to prioritise cybersecurity in the procurement process. In this use case / scenario the type of procurement is ‘Cloud services’.

4.2.2. Good practices for procurement

The procurement type is defined in Annex A, while the checklist in Annex B should be used to identify the relevant measures across the plan, source and manage phases. The following measures are an illustrative selection for this scenario.

General measures

General measures	
Group	**Objective**
GENERAL-03.06	Verify that cloud service suppliers are included in the supplier inventory with their security qualifications and contract terms noted.
GENERAL-07.07	Ensure cloud service-level agreements (SLAs) include disaster recovery and backup provisions, and that these are documented in procurement contracts.
GENERAL-08.06	Verify that cloud service supplier logs (access logs, administrator activity) are integrated into the hospital's or healthcare provider's monitoring and alerting processes.
GENERAL-09.02	Ensure ICT system, product or service supplier's commitments to GDPR-aligned data protection (confidentiality and integrity) are documented in procurement requirements.
GENERAL-09.03	Require the supplier to permanently erase or return all customer data (including backups) at contract end or upon retention-period expiry. Obtain documented termination procedures listing all assets and data to be returned or deleted, and verify deletion methods meet recognised secure-erasure standards.

Plan measures

Plan measures	
Group	**Objective**
PLAN-02.06	Verify that cloud procurement criteria include compliance with data security standards (e.g., ISO/IEC 27017/27018) and data residency requirements.
PLAN-06.01	Confirm that cloud contracts include data residency requirements (data stored in the specified jurisdiction, e.g., EU) to meet data sovereignty requirements.
PLAN-06.02	Ensure the contract obligates the cloud service supplier to use multiple geographically separated data centres, perform regular backups and support rapid failover for high availability.
PLAN-06.03	Verify that the contract specifies healthcare-specific security standards (e.g., ISO 27017/18, national health guidelines) and that the supplier aligns with NIS2 Directive incident reporting requirements.
PLAN-06.04	Ensure the contract gives the healthcare tenant control over encryption keys (where possible) and requires strong isolation between tenants.
PLAN-06.05	Ensure that the strategy defines the conditions that would trigger an exit (e.g., contract end, security breach, provider insolvency, unacceptable

Plan measures	
	performance) and that the procurement plan contains dedicated sections for 'Exit strategy' and/or 'Migration strategy'.
PLAN-06.06	Ensure that the contract includes a provision requiring the supplier to implement a documented process for the secure and verifiable deletion of all organisational data from its systems upon contract termination.
PLAN-06.07	Ensure that there is a procedure for the secure retrieval and export of all organisational data in a non-proprietary and usable format.

Source measures

Source measures	
Group	**Objective**
SOURCE-01.04	Verify that cloud service suppliers demonstrate comprehensive cybersecurity controls and are evaluated for secure design and operations.
SOURCE-02.06	Check that DPIA outcomes (e.g., data residency concerns) are captured in cloud service contracts and technical requirements.
SOURCE-03.02	Verify that the service contract / SLA includes quantitative security and availability metrics (e.g., defined uptime, capacity levels), timely incident-response and maintenance-notification clauses and explicit procedures for reporting security incidents
SOURCE-03.05	Require the cloud computing provider to describe its redundancy and business continuity measures (e.g., multi-zone failover) and to outline its security incident reporting process (e.g., NIS2-compliant notifications)
SOURCE-03.09	Require that the cloud service supplier implements strict logical segmentation between tenants at all layers (network, compute, storage) so that one customer's resources and data cannot be accessed by another. Obtain evidence of the supplier's tenant-isolation policies/configuration to verify proper segmentation.
SOURCE-03.10	Require the cloud service supplier to explicitly state data storage locations, ensuring patient data stays within approved jurisdictions (e.g., EU). The request for proposal (RFP) must also ask for a description of encryption mechanisms for data at rest and in transit (e.g., Advanced Encryption Standard (AES)-256, transport layer security (TLS)).
SOURCE-05.07	Check that cloud platforms or services being procured use secure infrastructure-as-code and that deployment configurations are integrity-checked.

Manage measures

Manage measures	
Group	**Objective**
MANAGE-01.04	Confirm that cloud service suppliers have defined patch management processes for reported vulnerabilities and that the organisation periodically reviews patch status.
MANAGE-03.03	Verify that cloud service suppliers have designated security contacts and clear definitions of reportable incidents, aligning with organisational policies. Definitions should be in alignment with entity incident definitions (where applicable for provided services).

4.3. Use case / Scenario 3: Procurement of off the shelf EHR system from a general practitioner

General practitioners usually practice medicine, without any additional staff other than their potential administrative assistant. These healthcare providers are not subject to the NIS2 directive and therefore are not required to comply with the respective cybersecurity requirements. Oftentimes they are also not aware of possible legal, regulatory or contractual requirements relating to cybersecurity.

4.3.1. Background

A general practitioner treats patients in her office, for a broad range of conditions and relies on digital tools to manage appointments, patient records and prescriptions. To enhance efficiency and to minimise the risk of losing patient data, the doctor is considering to procure an off the shelf, cloud-based core EHR system. This will allow her to store and process sensitive data and prescriptions, without having to maintain any specialised infrastructure.

Due to recent cyber attacks targeting medical data and their subsequent leak and/or unavailability, she would like to ensure that cybersecurity is considered throughout the procurement process. This will also maintain the doctor's reputation. As such, this use case / scenario relates to the type of procurement 'Clinical information systems'.

4.3.2. Good practices for procurement

The procurement type is defined in Annex A, while the checklist in Annex B should be used to identify the relevant measures across the plan, source and manage phases. The following measures are an illustrative selection for this scenario.

General measures

Measure	Description
GENERAL-03.02	Ensure the contract designates a 24/7 security contact point at the cloud service supplier with a guaranteed response time. Verify that the supplier will maintain an always-available contact (e.g., hotline or security operations centre email) for incident escalation.

Measure	Description
GENERAL-03.03	Check that security-related contract terms (e.g., patching, incident response) are documented for each key CIS ICT system, product or service supplier.
GENERAL-03.05	Ensure there is a process to escalate issues if a supplier's security posture degrades (e.g., hold orders, contract termination triggers).
GENERAL-06.07	Verify that ICT system, product or service suppliers or third-party access to CIS is restricted (pre-approved, scoped, time-limited) and uses secure authentication.
GENERAL-07.07	Ensure cloud service SLAs include disaster recovery and backup provisions, and that these are documented in procurement contracts.
GENERAL-09.02	Ensure ICT system, product or service providers' commitments to GDPR-aligned data protection (confidentiality and integrity) are documented in procurement requirements.
GENERAL-09.03	Require the provider to permanently erase or return all customer data (including backups) at contract end or upon retention-period expiry. Ensure data is transferred in open formats. Obtain documented termination procedures listing all assets and data to be returned or deleted, and verify deletion methods meet recognised secure-erasure standards.
GENERAL-09.04	Confirm that encryption is enforced for data in transit and at rest across all procured solutions, and that providers support strong cryptographic protocols.

Plan measures

Plan measures	
Group	**Objective**
PLAN-02.03	Confirm that RFPs for CIS specify compliance with healthcare data protection laws (GDPR), security standards (e.g., ISO/IEC 27001) and the CRA's framework, as indicated in Article 104 of the EHDS Regulation, where applicable.
PLAN-02.04	Verify that a compliance checklist (including NIS2 Directive incident reporting and GDPR requirements) is used during procurement evaluations. Suppliers are obligated to build in security from the earliest stages of development and to provide secure default configurations, especially concerning the integration of EHRs. If applicable, suppliers should provide an EU declaration of conformity declaring that the product meets all applicable EU health, safety and security requirements.
PLAN-04.01	Check that RFPs/requests for quotes include concrete cybersecurity requirements (data encryption at rest / in transit, MFA, audit logging).

Plan measures	
PLAN-04.02	Ensure procurement documents require ICT system, product or service suppliers to support the entire product life cycle with security updates and end-of-life plans.
PLAN-04.03	Verify RFPs include an incident response clause requiring ICT system, product or service suppliers to notify the procuring entity within 24 hours of any breach affecting the product or data.
PLAN-05.01	Confirm RFP security requirements reference relevant standards and regulations (e.g., NIS2 Directive, GDPR) and mandate evidence of compliance.
PLAN-06.01	Confirm that cloud contracts include data residency requirements (e.g., data stored within the EU) and explicitly restrict administrative and support access to personnel located within jurisdictions that meet equivalent data protection standards. Ensure that remote access from non-compliant regions is prevented or strictly controlled.
PLAN-06.03	Verify that the contract specifies healthcare-specific security standards (e.g., ISO 27017/18, national health guidelines) and that the supplier aligns with NIS2 Directive incident reporting requirements.
PLAN-06.05	Ensure that the strategy defines the conditions that would trigger an exit (e.g., contract end, security breach, provider insolvency, unacceptable performance) and that the procurement plan contains dedicated sections for ‘Exit strategy’ and/or ‘Migration strategy’.
PLAN-06.06	Ensure that the contract includes a provision requiring the supplier to implement a documented process for the secure and verifiable deletion of all organisational data from its systems upon contract termination.

Source measures

Source measures	
Group	**Objective**
SOURCE-01.03	Check that selection of CIS ICT system, product or service suppliers includes evaluation of their product certifications and security audit reports.
SOURCE-02.01	Confirm that a DPIA is performed or updated for any procured system processing sensitive health data, identifying privacy risks.
SOURCE-02.04	Check that the DPIA’s identified risks (e.g., cross-border data flow) are addressed through procurement safeguards (e.g., encryption, contractual terms).
SOURCE-02.08	Verify DPIA covers data collected or stored by mobile devices and that security requirements (e.g., device encryption) are enforced.

Source measures	
SOURCE-03.02	Verify that the service contract / SLA includes quantitative security and availability metrics (e.g., defined uptime, capacity levels), timely incident-response and maintenance-notification clauses, and explicit procedures for reporting security incidents
SOURCE-03.04	Define logging requirements in procurement documents (e.g., audit trails for access, retention periods) and confirm the supplier's systems meet them. Require the ICT system, product or service suppliers to enable secure central log export or off-site logging. Verify logs are tamper-resistant and sufficient for forensic analysis.
SOURCE-03.07	Ensure CIS of ICT system, product or service suppliers' access to systems is restricted (principle of least privilege) and only occurs through secure management channels with MFA.

Manage measures

Manage measures	
Group	**Objective**
MANAGE-03.01	Confirm that supplier contracts require immediate notification of any cybersecurity incident affecting their products or services.
MANAGE-05.01	Check that an asset inventory tracks the end-of-life of CIS equipment and that secure data disposal procedures (e.g., NIST 800-88 erasure) are applied.

Annex A: Types of procurement in healthcare

Types of procurement in healthcare	
Type of procurement	**Description**
CIS	Includes procurement of any kind of software oriented towards medical care: hospital information systems and EHR, laboratory information systems, radiology information and picture archiving and communication systems, pharmacy, drug databases, care management, diet or other disease and nutrition patient support software, computer physician order entry – big data analysis, etc., administrative IT systems and desktop computers used as endpoints. CIS must be located in the medical building or in a data centre facility under complete control of the IT division of the medical centre. Cloud-based systems have their own category.
Medical devices	Any piece of hardware/software dedicated to treatment, control or diagnosis of diseases: radiology equipment, radiotherapy, nuclear medicine, operative room or intensive care equipment, robots for surgery, electro-medical equipment, infusion pumps, spirometry devices, medical lasers, endoscopy equipment, IVDs used on biological samples, etc.

Types of procurement in healthcare	
	Includes patient implantable devices (holters, pacemakers, insulin pumps, cochlear implants, brain stimulators, cardiac defibrillators, gastric stimulators, etc.) ([29]) or wearables (external electrocardiograph or pressure holters, glucose monitors, etc.) that communicate by electronic means with the IT systems of the hospital.
Network equipment	Network lines (coaxial, optical), gateways, routers, switches, firewalls, VPN, intrusion prevention systems, intrusion detection systems, etc.
Remote care systems	Facilities or devices that deliver medical care outside the hospital environment, particularly services now referred to as 'hospital-based home care services', including telemedicine connected to the hospital. Can also include remote communication 'press-for-help' devices used to assist elderly individuals that live alone at home.
Mobile client devices	All pieces of software that provide health assistance or medical data collection not directly connected to the hospital network, for example, telemedicine apps. This does not include health wearables as they are included into a separate category. Mobile client devices need a defined protocol to connect to the hospital network.
Identification systems	Systems to uniquely identify patients or medical personnel (biometric scanners, card readers, etc.) and guarantee identification and/or authorisation to access IT systems.
Healthcare facility infrastructure	Any type of construction that can hold medical facilities. Includes electricity lines, water, gas, medical gases, furniture, etc., except network lines, which are included under the 'network equipment' category. BMS are included in the next procurement category as they are mainly control systems.
ICS/SCADA	Systems that control all physical aspects of the control centres such as power regulation systems, door lock systems, closed circuit security systems, heating, ventilation and air conditioning systems, alarm systems, water, heating, auxiliary power units, security access, elevators and fire extinguishing systems. Nowadays, control of all these systems is managed through software systems. BMS may be acquired separately or as part of a building renovation project.

([29]) Knee or hip replacements or intraocular lenses are also examples or 'medical devices' but are out of the scope of this study. For a detailed definition of 'medical device' see Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj). See also Tabasum, A., Safi, Z., Al Khater, W. and Shikfa, A, 'Cybersecurity issues in implanted medical devices', *2018 International Conference on Computer and Applications (ICCA)*, Institute of Electrical and Electronics Engineers, Beirut, Lebanon, 2018, pp. 1–9, https://doi.org/10.1109/COMAPP.2018.8460454.

Types of procurement in healthcare	
Professional services	All kind of services, outsourced or not, provided by professionals or companies: medical services, transportation, accounting, engineering, IT, legal, maintenance, cleaning, catering, etc.
Cloud services	Any CIS or other information system not located in the medical building or in a data centre facility under complete control of the IT division of the medical centre.
Managed security services	Outsourced security solutions provided by specialised ICT system, product or service suppliers, including continuous monitoring and management of cybersecurity infrastructure. Typically encompasses intrusion detection and prevention, security information and event management (SIEM), vulnerability assessment, security audits, endpoint protection, threat intelligence, incident response and compliance management.
Managed services	Outsourced management provided by external ICT system, product or service suppliers, covering operation, maintenance, monitoring and administration of systems and infrastructure. Managed services typically include network management, server and storage administration, backup and disaster recovery solutions, software updates and patch management, helpdesk support, user administration, database administration and performance optimisation.
System integrator services	Services provided by external ICT products or service suppliers or professional service suppliers that ensure seamless integration, interoperability and optimised performance of diverse information technology and clinical systems within healthcare facilities. System integration services include planning, design, installation, customisation, configuration, testing, training and support for integrated systems, such as hospital information systems, EHR systems, laboratory information systems, radiology information and picture archiving and communication systems, network infrastructure, security solutions, and other software and hardware platforms.
Web services	Any internet-based services or platforms enabling healthcare providers to deliver digital content, interactive communication or transactional capabilities to patients, healthcare professionals or external entities. Web services include patient portals, teleconsultation platforms, appointment scheduling systems, online billing and payment systems, health education portals, application programming interfaces for interoperability (Health Level Seven / Fast Healthcare Interoperability Resources (HL7/FHIR) compliant), interfaces for cloud-based platforms and/or patient engagement, and services leveraging standard internet protocols (Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), representational state transfer (RESTful) application programming interfaces (APIs)).
AI-enabled products	Any software or hardware solution leveraging AI techniques – including machine learning, natural language processing, deep learning and computer vision – to support clinical decision-making, patient care optimisation,

Types of procurement in healthcare	
	administrative workflows, predictive analytics and operational efficiency. AI-enabled products can include diagnostic imaging software, predictive analytics tools, patient triage solutions, virtual assistants, medical chatbots, robotic process automation, smart clinical documentation, personalised medicine applications and real-time monitoring systems.

Annex B: Checklists and prioritisation

This guide defines two levels of complexity of application for measures (level 1 and level 2), from a basic level to a high-assurance level for critical systems. Level 1 is for basic, low-assurance products and services and is easily testable, while level 2 is for products and services handling critical ([30]) processes and data.

The table metadata for each measure are:

a) code/identifier – specifies whether the measure is part of the hospital's or healthcare provider's strategic approach to ICT supply chain cybersecurity, or belongs to one of the three procurement phases;
b) description of the measure;
c) procurement type (see the list in Annex A);
d) level of complexity of application of the measure (level 1 being less complex, level 2 being more complex).

B.1. General (All phases)

Measure	Description	Procurement type	Levels
GENERAL-01.01	Verify the existence of a formal cybersecurity procurement policy, approved by executive management, covering risk management and supplier security (as mandated by the NIS2 Directive).	All procurement service types	Level 1
GENERAL-01.02	Confirm that every new procurement undergoes a documented cybersecurity risk assessment with management-approved risk treatment plans. Conduct a structured threat-identification process with relevant stakeholders (IT, clinical, legal) to identify and document risks introduced by the acquisition.	All procurement service types	Level 1

([30]) Based on confidentiality, integrity, authenticity and availability requirements, to indicate the protection required according to their sensitivity, criticality, risk and business value.

Measure	Description	Procurement type	Levels
GENERAL-01.03	Update the organisation's threat model for any new product or service being procured.	All procurement service types	Level 1
GENERAL-01.04	Verify that security and IT personnel (e.g., person acting as an information security lead) are integrated into procurement decision committees and that cybersecurity criteria are explicitly included in selection processes.	All procurement service types	Level 2
GENERAL-01.05	Check that the organisation's risk appetite for third-party products is defined and applied during supplier selection to ensure alignment with risk management policies.	All procurement service types	Level 2
GENERAL-02.01	Confirm that procurement budgets explicitly include funds for cybersecurity measures (secure technology, updates, certifications).	All procurement service types	Level 1
GENERAL-02.02	Verify that life cycle security costs (maintenance, support fees, patch management) are factored into initial and ongoing budgets rather than treated as optional.	All procurement service types	Level 1
GENERAL-02.03	Ensure resources for staff training on new systems and periodic security audits are budgeted as part of procurement planning.	All procurement service types	Level 1
GENERAL-02.04	Ensure periodic reviews of cybersecurity expenditures occur to adjust funding based on the evolving threat landscape and organisational needs.	All procurement service types	Level 2
GENERAL-03.01	Confirm that a detailed inventory of critical suppliers (e.g., CIS ICT system, product or service suppliers) and the products/services they provide is maintained and regularly updated.	Clinical information systems	Level 1
GENERAL-03.02	Ensure the contract designates a 24/7 security contact point at the cloud service supplier with a guaranteed response time. Verify that the supplier will maintain an always-available contact (e.g., hotline or security operations centre email) for incident escalation.	Clinical information systems, cloud services, network equipment, medical devices	Level 1

Measure	Description	Procurement type	Levels
GENERAL-03.03	Check that security-related contract terms (e.g., patching, incident response) are documented for each key CIS ICT system, product or service supplier.	Clinical information systems	Level 1
GENERAL-03.04	Verify that each CIS supplier is periodically re-evaluated (e.g., annual security questionnaire or audit) and records of these reviews are kept.	Clinical information systems	Level 2
GENERAL-03.05	Ensure there is a process to escalate issues if a supplier's security posture degrades (e.g., hold orders, contract termination triggers).	Clinical information systems	Level 2
GENERAL-03.06	Verify that cloud service suppliers are included in the supplier inventory with their security qualifications and contract terms noted.	Cloud services	Level 1
GENERAL-03.07	Confirm that network hardware suppliers are regularly monitored for security incidents and that updated assessment reports are obtained.	Network equipment	Level 2
GENERAL-03.08	Ensure that suppliers of medical equipment are evaluated for security posture as part of the supplier management programme.	Medical devices	Level 1
GENERAL-03.09	Check that all critical suppliers (for IT and services) are re-assessed on a scheduled basis and that significant changes in their security are addressed in contracts.	All procurement service types	Level 2
GENERAL-04.01	Verify that the organisation maintains an up-to-date inventory of all assets (including new procurements) and applies security patches or mitigations promptly for critical vulnerabilities.	All procurement service types	Level 1
GENERAL-04.02	Confirm that continuous vulnerability scanning and monitoring are performed for procured products, and that discovered vulnerabilities are tracked and addressed without undue delay.	All procurement service types	Level 1
GENERAL-04.03	Ensure there is a defined channel for reporting discovered vulnerabilities (from staff or suppliers) and that reported vulnerabilities follow a documented response procedure.	All procurement service types	Level 2

Measure	Description	Procurement type	Levels
GENERAL-04.04	Verify that a UDI-DI has been assigned to the device and is correctly documented, the intended purpose of the device is clearly defined, and a comprehensive description of the device, including variants and accessories, is available.	Medical devices	Level 2
GENERAL-04.05	Ensure contracts with suppliers require timely disclosure and patching of vulnerabilities, reflecting requirements set out in Article 21(e) of the NIS2 Directive.	All procurement service types	Level 2
GENERAL-05.01	Ensure that the patch management policy covers all critical systems and equipment and that security patches from ICT system, product or service suppliers are applied promptly according to schedule.	Medical devices, clinical information systems, network equipment, mobile client devices, identification systems, healthcare facility infrastructure, ICS/SCADA, remote care systems	Level 1
GENERAL-05.02	Verify that patching procedures include testing patches on non-production device samples and that any devices which cannot be patched have documented compensating controls.	Medical devices	Level 2
GENERAL-05.03	Verify that mitigating controls are implemented and documented for critical systems and equipment with vulnerabilities or limited patch support.	Clinical information systems, network equipment, mobile client devices, identification systems, healthcare facility infrastructure, ICS/SCADA, remote care systems	Level 2
GENERAL-06.01	Confirm that network segmentation is implemented to isolate critical medical networks and healthcare systems from general networks, limiting exposure.	Network equipment	Level 1
GENERAL-06.02	Confirm that medical device networks are isolated or on dedicated segments, preventing unauthorised access via general networks.	Medical devices	Level 1

Measure	Description	Procurement type	Levels
GENERAL-06.03	Check that ICS networks are separated from IT networks and that traffic to and from ICS/SCADA devices is strictly controlled.	ICS/SCADA, healthcare facility infrastructure	Level 1
GENERAL-06.04	Ensure least-privilege and MFA are required for accessing clinical information systems and that CIS networks are segregated from less-sensitive networks.	Clinical information systems	Level 1
GENERAL-06.05	Verify that network access controls (firewalls, access control lists) are configured to block unnecessary traffic and that network diagrams document segmentation zones.	Network equipment	Level 2
GENERAL-06.06	Ensure that MFA is enforced for accessing network management interfaces and that ICT system, product or service suppliers' default credentials are replaced.	Network equipment	Level 2
GENERAL-06.07	Verify that ICT system, product or service suppliers or third-party access to CIS is restricted (pre-approved, scoped, time-limited) and uses secure authentication.	Clinical information systems	Level 2
GENERAL-06.08	Verify that remote maintenance access to medical devices is strictly controlled (e.g., via VPN with MFA) and logged. One-time and time-limited sessions should be used, without the use of permanent accounts, as a condition for the procurement, with the possibility of refusing the offer in case of non-compliance. If remote access is not used regularly, it should be disabled and enabled only when necessary, and traffic should be encrypted.	Medical devices, remote care systems	Level 2
GENERAL-06.09	Ensure ICS/SCADA access (operator or ICT system, product or service suppliers) requires strong authentication (e.g., MFA or hardware tokens) and that sessions are monitored.	ICS/SCADA, healthcare facility infrastructure	Level 2
GENERAL-07.01	Confirm an up-to-date business continuity plan (BCP) exists for critical healthcare IT systems, defining roles, backups, failover and recovery procedures.	Clinical information systems	Level 1

Measure	Description	Procurement type	Levels
GENERAL-07.02	Ensure continuity plans address the availability of medical devices during outages (e.g., backup devices or manual alternatives).	Medical devices	Level 1
GENERAL-07.03	Check that ICS/SCADA BCP scenarios include manual control procedures or redundant systems for critical operations during cyber incidents.	Industrial control systems, healthcare facility infrastructure	Level 1
GENERAL-07.04	Verify that network infrastructure redundancy is included in the BCP (e.g., alternative connectivity) and that failover mechanisms are documented.	Network equipment	Level 1
GENERAL-07.05	Check that tests of device failover (e.g., backup procedures) are documented and result in updates to continuity planning.	Medical devices	Level 2
GENERAL-07.06	Confirm BCP testing covers network failure scenarios (e.g., switching to backup links) with documented outcomes and improvements.	Network equipment	Level 2
GENERAL-07.07	Ensure cloud service SLAs include disaster recovery and backup provisions, and that these are documented in procurement contracts.	Cloud services	Level 2
GENERAL-07.08	Verify that the BCP is regularly tested (e.g., drills for system recovery) and updated, and includes ICT system, product or service suppliers support obligations during outages. Suppliers should participate in BCP drills (where relevant and applicable)	Clinical information systems	Level 2
GENERAL-07.09	Verify that ICS/SCADA continuity drills (simulating outages) are performed and their results are used to improve recovery plans.	Industrial control systems, healthcare facility infrastructure	Level 2
GENERAL-08.01	Verify that a SIEM (or equivalent) is implemented to collect and correlate logs from all critical devices and applications, including managed security tools.	Managed security services	Level 1
GENERAL-08.02	Check that logging policies define which security-relevant events (logins, config changes) to record, and that logs are protected from tampering.	Managed security services	Level 1

Measure	Description	Procurement type	Levels
GENERAL-08.03	Ensure that network devices (e.g., firewalls, routers) forward logs to central monitoring and that significant events (e.g., denied access attempts) are tracked.	Network equipment	Level 2
GENERAL-08.04	Confirm that logs from clinical systems are forwarded to the SIEM and periodically reviewed by the security team for anomalies. When feasible, copy specific log files and use cases from the suppliers' firewall, infrastructure and SIEM to the organisation's SIEM.	Clinical information systems	Level 2
GENERAL-08.05	Check that event logs from medical devices are collected (if possible) and stored securely for later analysis.	Medical devices	Level 2
GENERAL-08.06	Verify that cloud logs (access logs, administrator activity) are integrated into the organisation's monitoring and alerting processes.	Cloud services	Level 2
GENERAL-09.01	Verify that any patient data handled by a new CIS is encrypted with modern algorithms (e.g., TLS1.3 in transit, AES-256 at rest) and that outdated protocols are disabled.	Clinical information systems	Level 1
GENERAL-09.02	Ensure ICT system, product or service providers' commitments to GDPR-aligned data protection (confidentiality and integrity) are documented in procurement requirements.	All procurement service types	Level 1
GENERAL-09.03	Require the provider to permanently erase or return all customer data (including backups) at contract end or upon retention-period expiry. Ensure data is transferred in open formats. Obtain documented termination procedures listing all assets and data to be returned or deleted, and verify deletion methods meet recognised secure-erasure standards.	All procurement service types	Level 1
GENERAL-09.04	Confirm that encryption is enforced for data in transit and at rest across all procured solutions, and that providers support strong cryptographic protocols.	All procurement service types	Level 1

Measure	Description	Procurement type	Levels
GENERAL-09.05	Check that cryptographic key management practices are robust (e.g., keys stored in hardware security modules, rotated periodically) for all new systems.	All procurement service types	Level 2
GENERAL-09.06	Verify that backups of critical data are encrypted and stored offline or offsite to prevent simultaneous compromise.	All procurement service types	Level 2
GENERAL-10.01	Check that organisation-wide cybersecurity training is provided to all staff (including procurement teams) and evaluated regularly.	All procurement service types	Level 1
GENERAL-10.02	Verify that specialised cybersecurity training is given to personnel in key roles (IT, developers, incident responders) as required by the NIS2 Directive.	All procurement service types	Level 1
GENERAL-10.03	Ensure that training for procurement and ICT system, product or service providers management includes assessing ICT system, product or service providers security claims and understanding NIS2 Directive requirements.	All procurement service types	Level 2
GENERAL-10.04	Confirm that third-party contractors and ICT system, product or service providers interacting with systems have completed equivalent security training or certification.	All procurement service types	Level 2
GENERAL-11.01	Confirm that security validation (e.g., penetration testing, audits, independent assessments) is performed on procured products or services before deployment. Ensure that the security of other service components is not compromised by new additions. When feasible, scan the external attack surface of both the general access to supplier and the specific solutions supplied, and perform own vulnerability scan of the internal components of the specific solutions supplied.	All procurement service types	Level 1

Measure	Description	Procurement type	Levels
GENERAL-11.02	Verify that systems provided by ICT system, product or service providers are authorised only after meeting the organisation's cybersecurity standards, based on security test results.	All procurement service types	Level 1
GENERAL-11.03	Ensure that there is a process for ongoing monitoring and periodic review of procured systems' security (updating risk assessments accordingly).	All procurement service types	Level 2

B.2. Plan phase

Measure	Description	Procurement type	Levels
PLAN-01.01	Confirm that a formal cybersecurity risk assessment is conducted before initiating any procurement, identifying specific threats and impacts of the new product or service.	All procurement service types	Level 1
PLAN-01.02	Verify that procurement decisions use risk assessment outputs to adjust controls or budgets (or cancel procurement if risk exceeds tolerance).	All procurement service types	Level 1
PLAN-01.03	Ensure that risk assessments include evaluation of how new systems will interact with legacy assets and mitigate identified integration risks.	All procurement service types	Level 2
PLAN-01.04	Check that the organisation's risk appetite is applied to procurement and that supply chain and third-party risks are explicitly assessed in the analysis.	All procurement service types	Level 2
PLAN-02.01	Ensure procurement documentation lists security and regulatory requirements (e.g., MDR, Health Insurance Portability and Accountability Act, GDPR) relevant to medical devices. Best practice is to request the MDS2 form from the device ICT system, product or service providers during procurement. The MDS2 provides a standardised security profile for the device and aids in risk assessment.	Medical devices	Level 1
PLAN-02.02	Check that ICT system, product or service providers' bids for medical devices include evidence of following accepted cybersecurity guidelines,	Medical devices	Level 1

Measure	Description	Procurement type	Levels
	regulations (e.g., MDR) and standards or relevant certifications (e.g., ISO 27001, IEC 62304).		
PLAN-02.03	Confirm that RFPs for CIS specify compliance with healthcare data protection laws (GDPR), security standards (e.g., ISO/IEC 27001) and the CRA's framework, as indicated in Article 104 of the EHDS Regulation, where applicable.	Clinical information systems, remote care systems	Level 1
PLAN-02.04	Verify that a compliance checklist (including NIS2 Directive incident reporting and GDPR requirements) is used during procurement evaluations. Suppliers are obligated to build in security from the earliest stages of development and to provide secure default configurations, especially concerning the integration of EHRs. If applicable, suppliers should provide an EU declaration of conformity declaring that the product meets all applicable EU health, safety and security requirements.	Clinical information systems	Level 2
PLAN-02.05	Ensure legal review validates that contracts include data protection clauses and breach notification obligations for device suppliers.	Medical devices, remote care systems	Level 2
PLAN-02.06	Verify that cloud procurement criteria include compliance with data security standards (e.g., ISO/IEC 27017/27018) and data residency requirements.	Cloud services	Level 2
PLAN-02.07	Check that AI products under procurement meet applicable security and privacy guidelines, including ethical AI frameworks and data protection laws.	AI-enabled products	Level 2
PLAN-02.08	Confirm that contracts for professional services include cybersecurity requirements (personnel vetting, confidentiality) consistent with organisational policies.	Professional services	Level 1
PLAN-03.01	Confirm a documented procurement supply chain security policy exists, defining roles and minimum cybersecurity criteria for suppliers.	Clinical information systems, medical devices, remote care systems, network equipment, AI-enabled products, industrial control	Level 1

Measure	Description	Procurement type	Levels
		systems, building management systems	
PLAN-03.02	Check that supplier eligibility criteria include cybersecurity baselines (approved encryption, operating system support, authentication methods) that potential suppliers must meet.	Clinical information systems, medical devices, remote care systems, network equipment, AI-enabled products, healthcare facility infrastructure	Level 1
PLAN-03.03	Verify that an approved supplier inventory is maintained, covering suppliers of critical assets and including their security qualifications.	Clinical information systems, medical devices, remote care systems, network equipment, AI-enabled products, ICS/SCADA, healthcare facility infrastructure	Level 2
PLAN-03.04	Ensure the supply chain policy mandates procurement only from authorised, trusted ICT system, product or service suppliers to prevent introducing compromised products.	Clinical information systems, medical devices, remote care systems, network equipment, AI-enabled products, ICS/SCADA, healthcare facility infrastructure	Level 2
PLAN-04.01	Check that RFPs/requests for quotes include concrete cybersecurity requirements (data encryption at rest / in transit, MFA, audit logging).	All procurement service types	Level 1
PLAN-04.02	Ensure procurement documents require ICT system, product or service suppliers to support the entire product life cycle with security updates and end-of-life plans.	All procurement service types	Level 1
PLAN-04.03	Verify RFPs include an incident response clause requiring ICT system, product or service suppliers to notify the procuring entity within 24 hours of any breach affecting the product or data.	All procurement service types	Level 2
PLAN-05.01	Confirm RFP security requirements reference relevant standards and regulations (e.g., NIS2 Directive, GDPR) and mandate evidence of compliance.	All procurement service types	Level 2

Measure	Description	Procurement type	Levels
PLAN-05.02	Check that supplier contracts explicitly require timely application of security patches and reporting of vulnerabilities to the healthcare provider.	All procurement service types	Level 1
PLAN-05.03	Verify incident notification clauses obligate ICT system, product or service suppliers to report any cybersecurity incident affecting the product or data within a defined time frame (e.g., 24–72 hours).	All procurement service types	Level 1
PLAN-05.04	Ensure contracts define ICT system, product or service suppliers' liability and require cyber insurance or indemnification in the event of a data breach caused by the supplier.	All procurement service types	Level 2
PLAN-05.05	Confirm that subcontracting is restricted: ICT system, product or service suppliers must get approval for any subcontractor and flow down security requirements to them.	All procurement service types	Level 2
PLAN-05.06	Verify contracts include secure offboarding terms: secure return/destruction of data and support continuation plans at contract end.	All procurement service types	Level 2
PLAN-06.01	Confirm that cloud contracts include data residency requirements (e.g., data stored within the EU) and explicitly restrict administrative and support access to personnel located within jurisdictions that meet equivalent data protection standards. Ensure that remote access from non-compliant regions is prevented or strictly controlled.	Cloud services	Level 1
PLAN-06.02	Ensure the contract obligates the cloud service supplier to use multiple geographically separated data centres, perform regular backups and support rapid failover for high availability.	Cloud services	Level 2
PLAN-06.03	Verify that the contract specifies healthcare-specific security standards (e.g., ISO 27017/18, national health guidelines) and that the supplier aligns with NIS2 Directive incident reporting requirements.	Cloud services	Level 2
PLAN-06.04	Ensure the contract gives the healthcare tenant control over encryption keys (where possible) and requires strong isolation between tenants.	Cloud services	Level 2

Measure	Description	Procurement type	Levels
PLAN-06.05	Ensure that the strategy defines the conditions that would trigger an exit (e.g., contract end, security breach, provider insolvency, unacceptable performance) and that the procurement plan contains dedicated sections for 'Exit strategy' and/or 'Migration strategy'.	Cloud services	Level 2
PLAN-06.06	Ensure that the contract includes a provision requiring the supplier to implement a documented process for the secure and verifiable deletion of all organisational data from its systems upon contract termination.		
PLAN-06.07	Establish whether there is a detailed procedure for the secure retrieval and export of all organisational data in a non-proprietary, usable format.	Cloud services	Level 2
PLAN-07.01	Confirm that a cross-functional procurement committee (IT, clinical, legal) is established to incorporate cybersecurity considerations into procurement decisions.	All procurement service types	Level 1
PLAN-07.02	Verify that cybersecurity priorities (e.g., system interoperability, auditing) are defined and agreed upon by stakeholders and aligned with operational goals.	All procurement service types	Level 1
PLAN-07.03	Ensure management receives appropriate cybersecurity risk-management training (in line with the NIS2 Directive) and that stakeholder workshops document NIS2 Directive requirements.	All procurement service types	Level 2
PLAN-07.04	Check that stakeholder inputs and decisions are documented in procurement records for transparency and auditability.	All procurement service types	Level 2

B.3. Source phase

Measure	Description	Procurement type	Levels
SOURCE-01.01	Check that ICT system, product or service supplier selection criteria prioritise suppliers with certified or independently assessed security postures.	Medical devices, remote care systems	Level 1

Measure	Description	Procurement type	Levels
SOURCE-01.02	Verify that evaluations of ICT system, product or service supplier bids include assessment of the supplier's cybersecurity practices and history of security incidents.	Medical devices, remote care systems	Level 1
SOURCE-01.03	Check that selection of CIS ICT system, product or service suppliers includes evaluation of their product certifications and security audit reports.	Clinical information systems	Level 1
SOURCE-01.04	Verify that cloud service suppliers demonstrate comprehensive cybersecurity controls and are evaluated for secure design and operations.	Cloud services	Level 1
SOURCE-01.05	Confirm that managed service suppliers are assessed for cybersecurity capabilities (e.g., security certifications, incident management) as part of ICT system, product or service suppliers' selection.	Managed services	Level 1
SOURCE-01.06	Ensure that managed security suppliers demonstrate proven monitoring and response processes, as evidenced by third-party audits or certifications.	Managed security services	Level 1
SOURCE-01.07	Confirm that for critical procurements, a supplier risk assessment is performed examining the ICT system, product or service supplier's cyber incident history and overall security governance.	Medical devices, remote care systems	Level 2
SOURCE-01.08	Ensure that ICT system, product or service suppliers' incident response plans are assessed for alignment with NIS2 Directive timelines (24-hour early warning, 72-hour notification) during selection.	Medical devices, remote care systems	Level 2
SOURCE-01.09	Ensure network equipment ICT system, product or service suppliers are vetted for strong supply chain security (e.g., hardware authenticity, secure firmware processes) before selection.	Network equipment	Level 2
SOURCE-01.10	Ensure that any critical device is correctly classified according to rules set out in Annex VIII to the MDR, with justification provided.	Medical devices	Level 2
SOURCE-02.01	Confirm that a DPIA is performed or updated for any procured system processing sensitive health data, identifying privacy risks.	Clinical information systems	Level 1

Measure	Description	Procurement type	Levels
SOURCE-02.02	Confirm DPIA includes web-based applications (e.g., patient portals) and enforces privacy-enhancing measures (e.g., HTTPS, session security).	Web services	Level 1
SOURCE-02.03	Ensure DPIAs consider identification systems storing personal data and incorporate mitigations (e.g., data minimisation) into procurement requirements.	Identification systems	Level 1
SOURCE-02.04	Check that the DPIA's identified risks (e.g., cross-border data flow) are addressed through procurement safeguards (e.g., encryption, contractual terms).	Clinical information systems	Level 2
SOURCE-02.05	Verify that DPIA findings for identification systems result in specific procurement conditions (e.g., encryption, restricted access) to mitigate privacy risks.	Identification systems	Level 2
SOURCE-02.06	Check that DPIA outcomes (e.g., data residency concerns) are captured in cloud service contracts and technical requirements.	Cloud services	Level 2
SOURCE-02.07	Ensure DPIAs for AI products identify algorithmic or privacy impacts and that procurement includes controls (e.g., explainability, bias mitigation) as needed.	AI-enabled products	Level 2
SOURCE-02.08	Verify DPIA covers data collected or stored by mobile devices and that security requirements (e.g., device encryption) are enforced.	Mobile client devices	Level 2
SOURCE-03.01	Ensure procurement requires strict access controls for ICT system, product or service suppliers' maintenance (pre-approved, scoped access with MFA).	Medical devices, remote care systems	Level 1
SOURCE-03.02	Verify that the service contract / SLA includes quantitative security and availability metrics (e.g., defined uptime, capacity levels), timely incident-response and maintenance-notification clauses, and explicit procedures for reporting security incidents	Cloud services, managed services	Level 1

Measure	Description	Procurement type	Levels
SOURCE-03.03	Verify that all ICT system, product or service suppliers' maintenance and updates on devices are performed over secure, encrypted channels (e.g., VPN with MFA) and signed digital delivery.	Medical devices, remote care systems	Level 1
SOURCE-03.04	Define logging requirements in procurement documents (e.g., audit trails for access, retention periods) and confirm the supplier's systems meet them. Require the ICT system, product or service suppliers to enable secure central log export or off-site logging. Verify logs are tamper-resistant and sufficient for forensic analysis.	All procurement service types	Level 1
SOURCE-03.05	Require the cloud computing provider to describe its redundancy and business continuity measures (e.g., multi-zone failover) and to outline its security incident reporting process (e.g., NIS2-compliant notifications)	Cloud services	Level 1
SOURCE-03.06	Check that managed service suppliers access follows secure, multi-factor authenticated channels and that credentials cannot be reused beyond their intended purpose.	Managed services	Level 2
SOURCE-03.07	Ensure CIS of ICT system, product or service suppliers' access to systems is restricted (principle of least privilege) and only occurs through secure management channels with MFA.	Clinical information systems	Level 2
SOURCE-03.08	Verify that updates for network devices are delivered via encrypted, authenticated channels and require signing by the ICT system, product or service suppliers.	Network equipment	Level 2
SOURCE-03.09	Require that the cloud service supplier implements strict logical segmentation between tenants at all layers (network, compute, storage) so that one customer's resources and data cannot be accessed by another. Obtain evidence of the supplier's tenant-isolation policies/configuration to verify proper segmentation.	Cloud services	Level 2
SOURCE-03.10	For cloud procurements, require the supplier to explicitly state data storage locations, ensuring patient data stays within approved jurisdictions (e.g.,	Cloud services	Level 2

Measure	Description	Procurement type	Levels
	EU). The RFP must also ask for a description of encryption mechanisms for data at rest and in transit (e.g., AES-256, TLS).		
SOURCE-03.11	Confirm that ICT system, product or service suppliers must use secure remote maintenance methods (e.g., time-limited VPN) and apply MFA for any access.	ICS/SCADA, healthcare facility infrastructure	Level 2
SOURCE-03.12	Prioritise certified ICT products.	Medical devices, remote care systems, network equipment, AI-enabled products, ICS/SCADA, healthcare facility infrastructure	Level 2
SOURCE-03.13	Ensure manufacturers provide security documentation as part of device procurement.	Medical devices, remote care systems, network equipment, AI-enabled products, ICS/SCADA, healthcare facility infrastructure	Level 2
SOURCE-04.01	Ensure procurement specifies that hardware must be obtained directly from authorised manufacturers or certified distributors to guarantee authenticity.	Medical devices	Level 1
SOURCE-04.02	For devices with software, ensure that software validation has been performed following IEC 62304.	Medical devices	Level 1
SOURCE-04.03	Verify that firmware and software for network devices are delivered with checksums or digital signatures, and these are validated before installation.	Network equipment	Level 1
SOURCE-04.04	Check that suppliers provide digital signatures or device certificates for critical equipment ([31]) (e.g., first-boot firmware integrity).	Medical devices	Level 2
SOURCE-04.05	Confirm requirements that network gear support factory firmware integrity checks or signed updates to detect tampering.	Network equipment	Level 2

([31]) In line with the entity's risk assessment.

Measure	Description	Procurement type	Levels
SOURCE-04.06	Ensure that CIS software procurement requires verifying distribution authenticity (e.g., signed updates, checksums) to prevent tampering.	Clinical information systems	Level 2
SOURCE-04.07	Verify that ICS/SCADA component procurement mandates certified supply chains and code signing for firmware, in line with sector best practices.	ICS/SCADA, healthcare facility infrastructure	Level 2
SOURCE-05.01	Verify that suppliers of procured systems follow secure development practices (e.g., devices designed in line with the MDR with hardware security features).	Medical devices	Level 1
SOURCE-05.02	Ensure that procured web applications apply secure development (input validation, signed updates) and have undergone security reviews.	Web services	Level 1
SOURCE-05.03	Check that mobile apps used in procured solutions adhere to secure coding (no hardcoded credentials, encrypted storage) and have passed code review.	Mobile client devices	Level 2
SOURCE-05.04	Confirm that remote care solutions use signed updates and have intrusion detection, reflecting secure SDLC requirements.	Remote care systems	Level 2
SOURCE-05.05	Verify that CIS software includes automated and manual security code reviews and robust authentication mechanisms as part of procurement expectations.	Clinical information systems	Level 2
SOURCE-05.06	Ensure AI products under procurement implement secure machine-learning practices (e.g., validated inputs) and are produced in line with secure SDLC guidelines.	AI-enabled products	Level 2
SOURCE-05.07	Check that cloud platforms or services being procured use secure infrastructure-as-code and that deployment configurations are integrity-checked.	Cloud services	Level 2
SOURCE-05.08	Confirm that new identification/authentication devices are manufactured with tamper protection and no exposed debug interfaces, in line with secure development practices.	Identification systems	Level 2

Measure	Description	Procurement type	Levels
SOURCE-06.01	Check that ICT system, product or service suppliers' contracts include clauses for timely vulnerability disclosure and patching.	Medical devices	Level 1
SOURCE-06.02	Ensure that agreements with ICT system, product or service suppliers include penalties or corrective measures for failure to remediate critical vulnerabilities promptly.	Remote care systems	Level 2

B.4. Manage phase

Measure	Description	Procurement type	Levels
MANAGE-01.01	Verify that supplier contracts enforce the ICT system, product or service supplier's responsibility to receive vulnerability reports and provide fixes without undue delay.	Medical devices, remote care systems	Level 1
MANAGE-01.02	Check that a process exists to regularly monitor suppliers' security advisories and security bulletins related to deployed products.	Medical devices, remote care systems	Level 1
MANAGE-01.03	Ensure supplier-issued patches are integrated into the organisation's patch management workflow and that patch status is tracked for CIS products.	Clinical information systems	Level 2
MANAGE-01.04	Confirm that cloud service suppliers have defined patch management processes for reported vulnerabilities and that the organisation periodically reviews patch status.	Cloud services	Level 2
MANAGE-01.05	Verify that any critical network device vulnerabilities are reported to the ICT system, product or service suppliers and that evidence of patch deployment is recorded for audit.	Network equipment	Level 2
MANAGE-01.06	Check that ICS/SCADA suppliers treat security patches as high priority and coordinate updates in line with the organisation's maintenance schedule.	ICS/SCADA, healthcare facility infrastructure	Level 2
MANAGE-02.01	Verify that an asset inventory (including configurations) is maintained for all IT assets and that secure baselines are defined for new systems.	Managed services	Level 1

Measure	Description	Procurement type	Levels
MANAGE-02.02	Ensure maintenance agreements require suppliers to perform timely and secure updates (authorised tools, agreed procedures) and provide maintenance reports.	Managed services	Level 1
MANAGE-02.03	Check that third-party maintenance uses only pre-approved tools and methods, with logs or reports demonstrating adherence to technical security requirements.	Managed services	Level 2
MANAGE-02.04	Confirm that maintenance tasks on medical devices (updates, part replacements) are documented and performed using secure procedures.	Medical devices	Level 2
MANAGE-02.05	Verify that network equipment maintenance follows strict security procedures (e.g., no default tools) and is logged for audit purposes.	Network equipment	Level 2
MANAGE-02.06	Check that remote care device maintenance by ICT system, product or service suppliers uses secure channels and any change requests are reviewed for security impact.	Remote care systems	Level 2
MANAGE-02.07	Ensure ICS/SCADA maintenance (software updates, calibrations) uses secure processes and is scheduled to minimise risk, with verification of actions taken.	ICS/SCADA	Level 2
MANAGE-03.01	Confirm that supplier contracts require immediate notification of any cybersecurity incident affecting their products or services.	Managed services	Level 1
MANAGE-03.02	Confirm that managed security service suppliers promptly report detected incidents to the healthcare organisation, in line with NIS2 Directive reporting requirements. When feasible and needed, the organisation should add their own network detection and response units to the specific solutions supplied	Managed security services	Level 1
MANAGE-03.03	Verify that cloud service suppliers have designated security contacts and clear definitions of reportable incidents, aligning with organisational policies. Definitions should be in alignment with entity incident definitions (where applicable for provided services).	Cloud services	Level 1

Measure	Description	Procurement type	Levels
MANAGE-03.04	Ensure there is an established reporting mechanism (e.g., email, hotline) for ICT system, product or service suppliers to inform the hospital or the healthcare provider of security incidents.	Medical devices, remote care systems	Level 2
MANAGE-03.05	Check that supplier-reported incidents are treated as internal incidents (logged, triaged) and included in the formal incident response process.	Clinical information systems	Level 2
MANAGE-04.01	Verify that the organisation subscribes to threat intelligence feeds and participates in sector-specific information-sharing networks (e.g., health sector Information Sharing and Analysis Centre).	All procurement service types	Level 1
MANAGE-04.02	Ensure risk assessments of procured systems are reviewed and updated at least annually or after significant incidents, as required by continuous improvement practices.	All procurement service types	Level 1
MANAGE-04.03	Check that after-action (post-incident) reviews are used to refine cybersecurity measures, and that these improvements are documented and applied to procurement processes.	All procurement service types	Level 2
MANAGE-04.04	Confirm the organisation evaluates and adopts new cybersecurity tools (e.g., AI-based analytics) as part of its ongoing improvement process.	All procurement service types	Level 2
MANAGE-05.01	Check that an asset inventory tracks the end-of-life of CIS equipment and that secure data disposal procedures (e.g., NIST 800-88 erasure) are applied.	Clinical information systems	Level 1
MANAGE-05.02	Verify that data is securely erased from CIS hardware before disposal and that disposal actions are documented (certificates of destruction).	Clinical information systems	Level 1
MANAGE-05.03	Ensure that patient data on decommissioned medical devices is sanitised using certified tools and that devices are tracked to prevent unauthorised reuse.	Medical devices, remote care systems	Level 1

Measure	Description	Procurement type	Levels
MANAGE-05.04	Confirm that disposal of medical device hardware follows defined procedures and that asset records are updated when devices are destroyed or recycled.	Medical devices, remote care systems	Level 2
MANAGE-05.05	Verify that retired network equipment has its configurations wiped and storage media destroyed to prevent data leaks.	Network equipment	Level 2
MANAGE-05.06	Check that decommissioning of identification systems (e.g., badge readers) includes erasing user data and updating asset inventory.	Identification systems	Level 2

TP-01-26-017-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union

978-92-9204-804-4