



# PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS

Good practices for the security of Healthcare services

FEBRUARY 2020

# ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at [www.enisa.europa.eu](http://www.enisa.europa.eu)

## CONTACT

For contacting the authors please use [eHealthSecurity@enisa.europa.eu](mailto:eHealthSecurity@enisa.europa.eu)

For media enquiries about this paper, please use [press@enisa.europa.eu](mailto:press@enisa.europa.eu)

## AUTHORS

Dr. Athanasios Drougkas, Dimitra Liveri, Antigone Zisi, Pinelopi Kyranoudi

## ACKNOWLEDGEMENTS

For providing valuable information that helped shape the report (in alphabetical order):

Tomáš Bezouška, Ministry of Health, Czech Republic

Konstantinos Chondropoulos, Administration of the 3rd Health District of Macedonia, Greece

Dimitrios Glynos, Census Labs, Greece

Manuel Jimber Rio, Andalusian Healthcare Service, Spain

Dr. Luis Marti-Bonmati, Hospital Universitari i Politècnic La Fe, Spain

Dr. Julio Mayol, Hospital Clínico San Carlos, Spain

Dr. Germán Seara, Hospital Clínico San Carlos, Spain

Elena Sini, Humanitas Research Hospital, Italy

Centro Criptológico Nacional, Spain

## LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.

This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.



## COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2020

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN 978-92-9204-312-4, DOI 10.2824/943961



# TABLE OF CONTENTS

<b>1. INTRODUCTION</b>	<b>7</b>
1.1 OBJECTIVES	7
1.2 SCOPE	7
1.3 TARGET AUDIENCE	7
1.4 METHODOLOGY	8
1.5 POLICY CONTEXT	8
1.5.1 European Policy	8
1.5.2 International Policy	9
1.6 STRUCTURE OF THE REPORT	10
<b>2. PROCUREMENT IN HOSPITALS</b>	<b>11</b>
2.1 PROCUREMENT PROCESS	11
2.2 TYPES OF PROCUREMENT	13
2.3 RELEVANT INDUSTRY STANDARDS AND GUIDELINES	15
2.4 CYBERSECURITY CHALLENGES	18
<b>3. CYBERSECURITY IN PROCUREMENT</b>	<b>20</b>
3.1 THREAT TAXONOMY	20
3.1.1 Natural phenomena	22
3.1.2 Supply chain failure	22
3.1.3 Human errors	22
3.1.4 Malicious actions	23
3.1.5 System failures	25
3.2 RISKS IN PROCUREMENT	26
<b>4. GOOD PRACTICES FOR CYBERSECURITY IN PROCUREMENT</b>	<b>28</b>
4.1 GENERAL PRACTICES	29
4.2 PLAN PHASE PRACTICES	35
4.3 SOURCE PHASE PRACTICES	39
4.4 MANAGE PHASE PRACTICES	44

<b>5. OUTLOOK</b>	<b>46</b>
<b>A ANNEX: INDUSTRY STANDARDS</b>	<b>47</b>



# EXECUTIVE SUMMARY

As cybersecurity becomes more of a priority for hospitals, it is essential that it is integrated holistically in the different processes, components and stages influencing the healthcare ICT ecosystem. Procurement is a key process shaping the ICT environment of modern hospitals and, as such, should be at the forefront when it comes to meeting cybersecurity objectives.

This report aims to provide hospital procurement officers and CISOs/CIOs with a comprehensive set of tools and good practices that can be adapted to the hospitals' procurement process in order to ensure that cybersecurity objectives are met. In this context, the report maps good practices in three distinct phases comprising the procurement lifecycle, namely **plan**, **source** and **manage**. Indeed, cybersecurity considerations are relevant for all three phases and this report offers an easy-to-use guide for hospitals to improve their procurement process from a cybersecurity perspective.

This report provides the context for addressing cybersecurity in procurement by defining the three procurement phases, identifying 10 types of procurement (assets, products, services etc.) for which cybersecurity considerations are relevant, lists industry standards with cybersecurity aspects relevant to these types of procurement and highlights the main respective cybersecurity challenges. A threat taxonomy and a list of key risks associated with procurement are also presented. All this information is accompanied by quick guides providing insights as to how hospitals can use it in their procurement process.

The report concludes with a comprehensive set of good practices (GP) for cybersecurity in procurement. These good practices can be general practices applicable throughout the procurement lifecycle or may be relevant to individual procurement phases. All good practices are linked to types of procurement for which they are relevant and to threats which they can mitigate, providing an easy to filter set of practices for hospitals who want to focus on particular aspects. Overall, hospitals are encouraged to adopt these good practices for cybersecurity in procurement:

- **General practices:**

- **Involve the IT department** in procurement
- **Vulnerability management**
- Develop a policy for **hardware and software updates**
- Secure **wireless communication**
- Establish **testing policies**
- Establish **Business Continuity plans**
- Consider **interoperability** issues
- Allow **auditing and logging**
- Use **encryption**

- **Plan phase:**

- Conduct **risk assessment**
- Plan **requirements in advance**
- Identify **threats**
- **Segregate network**
- Establish **eligibility criteria** for suppliers
- Create **dedicated RfP for cloud**

- **Source phase**

- Require **certification**
- Conduct **DPIA**

- Address **legacy systems**
- Provide **cybersecurity training**
- Develop **incident response plans**
- Involve **supplier in incident management**
- Organise **maintenance operations**
- Secure **remote access**
- Require **patching**
- **Manage phase**
  - Raise **cybersecurity awareness**
  - Perform **asset inventory** and **configuration management**
  - Dedicated **access control** mechanisms for medical device facilities
  - Schedule **penetration testing** frequently or after a change in the architecture/  
system



# 1. INTRODUCTION

Healthcare is becoming increasingly connected, as medical technology companies currently manufacture more than 500,000 different types of medical devices, such as wearables, implantable and stationary medical devices<sup>1</sup>. The Internet of Medical Things market in Europe alone is expected to grow from 11 billion in 2017 to 40 billion in 2022, while the European medical technology market was estimated at roughly 115 billion in 2017<sup>2</sup>. At the same time, a study showed that U.S. hospitals had, on average, between 10 and 15 connected devices per bed, exemplifying how the proliferation of medical technology solutions has completely changed the ICT landscape in healthcare organisations worldwide. All these devices are made by different manufacturers, and all must effectively communicate with each other to deliver patient care. The increasing interconnection of medical devices and the use of remote connections for their maintenance; the need to continuously monitor the patients -even the ones out of the hospital; the use of smartphones to access health information by patients and doctors; along with the inability of the information technology (IT) department to apply patches and the usual lack of budget for cybersecurity services and solutions, make the healthcare sector especially vulnerable<sup>3</sup>. Cybersecurity should be considered in the early days of purchasing assets (infrastructure, software, systems, devices etc.) for healthcare organisations.

## 1.1 OBJECTIVES

This study focuses on one part of the vast healthcare ecosystem: the hospital. The hospital is considered as a collection of assets (infrastructure, software, systems, devices etc.), and cybersecurity should be explicitly addressed in all its different components. Overall, the objective of this study, is to provide healthcare professionals in hospitals with guidelines on how to improve their procurement process to meet cybersecurity objectives. These guidelines cover multiple topics and range from good organisational practices for the healthcare organisations themselves, up to what information to request from suppliers as cybersecurity “evidences” when procuring systems and services.

## 1.2 SCOPE

The scope of this study is on hospitals: the most complex and critical healthcare organisations and the main stakeholder for procurement. Also hospitals often face lack of resources, so this report aims at being a “guidebook” for healthcare professionals. Many of the practices and recommendations will be useful to other healthcare organisations as well, as procurement processes can be very similar. The procurement guidelines proposed in this report cover the entire procurement scope of healthcare organisations that can potentially impact cybersecurity.

## 1.3 TARGET AUDIENCE

This report is addressed to healthcare professionals occupying technical positions in hospitals, i.e. Chief-level executives: CIO<sup>4</sup>, CISO, CTO, IT teams as well as procurement officers in healthcare organisations.

This report may be of interest to manufacturers of medical devices that provide products to hospitals; in this case products can be (but are not limited to) medical devices, clinical information systems, networking equipment, cloud services, etc. When these manufacturers

**During the Wannacry attack in 2017, a ransomware spread exponentially, taking advantage of a vulnerability present only in 5% of the UK National Healthcare System (NHS) computers, which were still running outdated and unsupported software.**

<sup>1</sup> <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf>

<sup>2</sup> <https://www.medtecheurope.org/wp-content/uploads/2019/04/The-European-Medical-Technology-Industry-in-figures-2019-1.pdf>

<sup>3</sup> Lynne Coventry and Dawn Branley, 'Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward', *Maturitas* 113 (July 2018): 48–52, <https://doi.org/10.1016/j.maturitas.2018.04.008>.

<sup>4</sup> Chief Information Officer – CIO, Chief Information Security Officer – CISO, Chief Technology Officer – CTO etc





offer services or products, they will know the security requirements that the hospital expects them to fulfil and they can provide evidence to prove it.

## 1.4 METHODOLOGY

Information presented in this report is the result of analysis of data received through a series of interviews. The interviews were conducted with subject matter experts from hospitals, policy makers or regulators (ministries of health), medical device manufacturers and cybersecurity experts with a focus in healthcare. The report was validated by the experts participating in the survey/interviews, as well as with the ENISA eHealth Security Experts Group<sup>5</sup>.

This methodology enabled ENISA to engage actively with the interested stakeholders and:

- identify the types of procurement and corresponding assets with relevance to the hospitals' cybersecurity objectives,
- identify possible threats, risks and challenges related to procurement in hospital organisations,
- list good practices related to healthcare procurement in order to meet cybersecurity objectives, and
- map the proposed good practices to types of procurement for which they may be used and to threats for which they are relevant.

## 1.5 POLICY CONTEXT

### 1.5.1 European Policy

Legislation plays a major role in defining the cybersecurity requirements that should be described in the technical specifications when obtaining products and services in a hospital. Some of the most prominent are presented below:

#### 1.5.1.1 The Network and Information Security Directive (NISD)

The Network and Information Security Directive (NISD) 2016/1148/EU, which came into force in May 2018, has two main goals: the implementation of minimum security requirements and the establishment of cybersecurity notifications for both Operators of Essential Services and Digital Service Providers. Healthcare providers, namely hospitals, are identified as Operators of Essential Services in most Member States. Therefore, these organizations will have to take into account the Directive and the respective national law when contracting a product or service.

The Directive goes beyond implementation of security requirements, as it gives power to the regulatory bodies to audit the Operators of Essential Services to ensure the level of cybersecurity in the organization is acceptable and as per the provisions of the Directive. In the hospital ecosystems, this can be translated as cybersecurity requirements for all the products so it should be included as a provision in the procurement process. One vulnerable device/system/service can result into great cybersecurity impact for the hospital as an operator of essential service.

#### 1.5.1.2 Medical Device Regulation (MDR)

The Medical Device Regulation (MDR) is a new regulation that includes specific provisions related to the IT security (hardware, software etc.) for all medical devices. The General Safety and Performance Requirements defined within the MDR (Medical Devices/SW) include:

- repeatability, reliability and performance according to the intended use
- the principles of development life cycle, risk management, verification and validation
- the use of software in combination with mobile computing platforms

**European legislation introduces a notification obligation to the hospitals. In some cases the notification should follow the supply chain. This has to be foreseen during the procurement process.**

<sup>5</sup> <https://resilience.enisa.europa.eu/ehealth-security>

- IT security measures, including protection against unauthorised access

### 1.5.1.3 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR)<sup>6</sup> came into force on 25 May 2018. It sets the rules for the processing and free movement of personal data and applies to all domains of the public and private sector; however, some specific derogations are defined for data concerning health, aiming at protecting the rights of data subjects and confidentiality of their personal health data and at the same time preserving the benefits of data processing for research and public health purposes.

GDPR treats health data as a "special category" of personal data which are considered to be sensitive by nature and imposes a higher standard of protection for their process. Organizations processing health data have the following obligations (among others):

- to implement appropriate technical and organisational measures to ensure security of the processing systems, services and personal data,
- to perform data protection impact assessment, and
- to report data breaches which are likely to result in a risk to the rights and freedoms of individuals within 72 hours after having become aware of.

Article 4 (12) of the GDPR defines a "personal data breach" as a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed; It has to be noted that if a data breach incident impacts the continuity of the health services as well, then it has to be reported according to the NIS Directive.

## 1.5.2 International Policy

### 1.5.2.1 Health Insurance Portability and Accountability Act of 1996 (HIPAA)<sup>7</sup>

This Act required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI).

### 1.5.2.2 FDA Guidance for cybersecurity<sup>8</sup>

This guidance has been developed by the FDA to assist industry by identifying issues related to cybersecurity that manufacturers should address in the design and development of their medical devices as well as in preparing premarket submissions for those devices.

If a manufacturer would aim for internal markets, then the device should comply with both European and international law.

---

<sup>6</sup> REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

<sup>7</sup> <https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm>

<sup>8</sup> <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices>

## 1.6 STRUCTURE OF THE REPORT

The study is structured as follows:

[Section 2](#): Definition of the context around Healthcare Procurement Processes and its variants with an overview of the concepts discussed and the related security challenges.

[Section 3](#): Threat and risk analysis containing a taxonomy of the threats and examples of Healthcare sector attack scenarios.

[Section 4](#): Description of good procurement practices mapped to threats and types of procurement.

Annex A: List of relevant industry standards

*Each section of the report is accompanied by a description of how hospitals can use the information provided in the section to address cybersecurity in their procurement processes. The relevant descriptions are given in text boxes such as this one.*

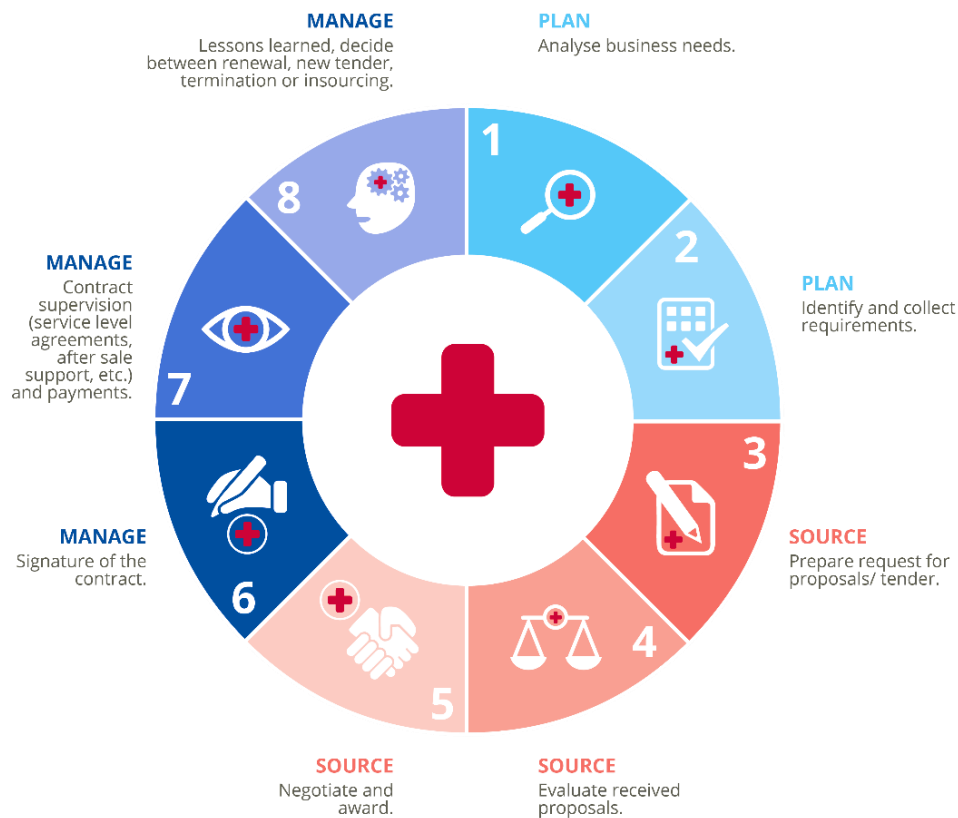
# 2. PROCUREMENT IN HOSPITALS

## 2.1 PROCUREMENT PROCESS

*Understand where cybersecurity fits in the different phases of the procurement lifecycle. This section indicates what cybersecurity considerations should be addressed when planning procurement, in the source process and in the post-sales/manage phases.*

Since the hospital ecosystem is comprised by several IT components, cybersecurity should be examined separately in all these different components. Cybersecurity should be part of all different stages of the procurement process. In this section, we present the common stages of the procurement process for obtaining products and services (including medical devices, information systems and infrastructures), together with some considerations as per each stage of the process.

**Figure 1: Procurement process lifecycle for hospitals**



- Plan phase: Initially, the hospital analyses its needs and collects requirements from several divisions internally. For example, in the case of obtaining a new cloud service, the CTO should identify the needs and understand what kind of usability this service will offer.
- Source phase: Afterwards, the requirements are translated into technical specifications and, in collaboration with the procurement office, the sourcing process begins (e.g., a tender is published). The hospital receives the designated offers, the committee (including the CTO/ CISO or and member of the IT team) evaluates the offers and selects the most appropriate products. Negotiations are conducted with the contractor and the contract is awarded.
- Manage phase: Finally, the contract (management and monitoring) is assigned to the business owner within the hospital. The assigned officer is responsible for closing the tender and receiving any feedback from users on the actual performance of the equipment/system/service.

Throughout the different phases of the procurement lifecycle, the hospital should ensure cybersecurity is considered as a requirement for the product/service to be procured. Relevant considerations may include:

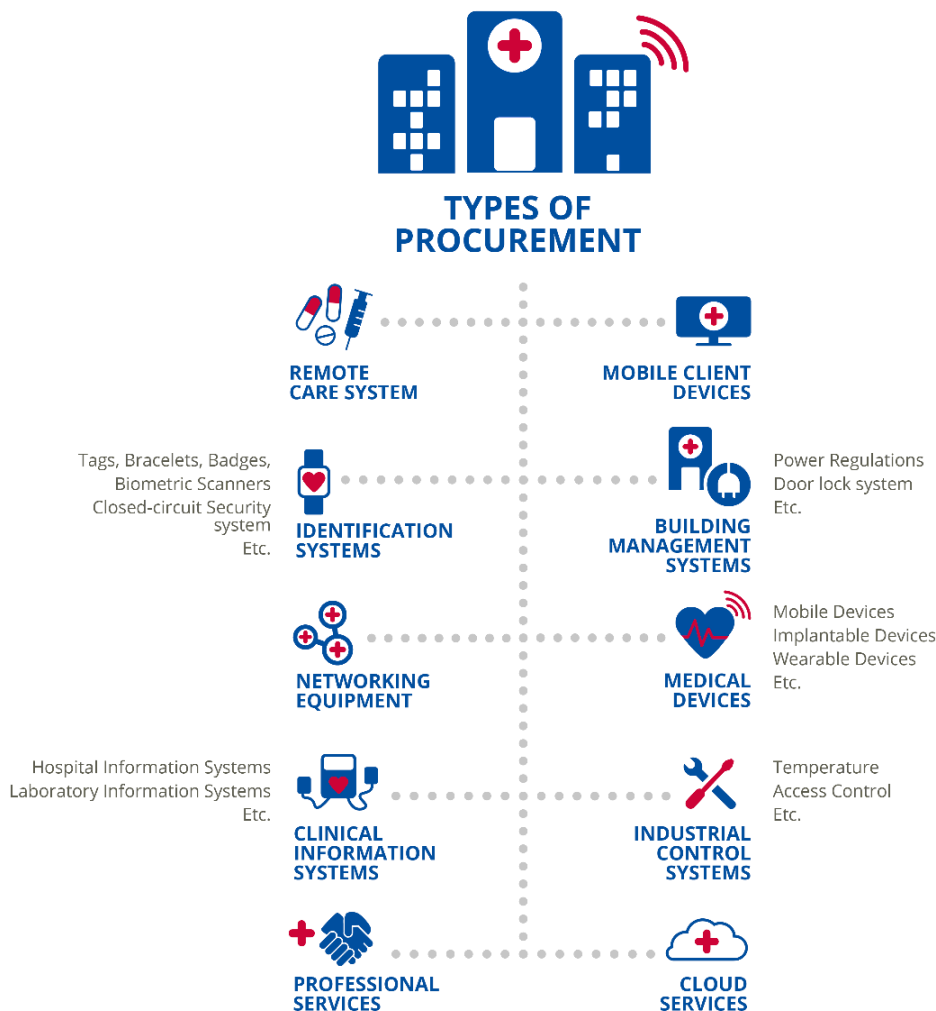
- Plan phase: The cybersecurity risks associated with a new procurement are assessed and specific cybersecurity requirements for the new procurement are defined.
- Source phase: Cybersecurity requirements are translated into technical specifications and product security features and supplier responsibilities for cybersecurity aspects are clarified and included in the contracts.
- Manage phase: Cybersecurity aspects, such as incidents and new vulnerabilities are continuously monitored and corrective measures, such as patching are applied to maintain a high level of security. Similarly, at the end of the products lifecycle, secure disposal is required for privacy reasons as devices have patient information stored.

## 2.2 TYPES OF PROCUREMENT

*Cybersecurity considerations are relevant for a number of different types of procurement. Consult the following list to understand if the specific type of procurement you are planning/managing has possible cybersecurity implications that should be addressed.*

As discussed throughout this document, the hospital is an ecosystem comprised by several components and cybersecurity should be a priority for all these different components. In this chapter we created a taxonomy to categorise the types of procurement and eventually investigate how cybersecurity is addressed in each type.

**Figure 2: Types of procurement (asset taxonomy)**



**Table 1: Types of procurement**

Type of procurement	Type description
<b>Clinical information systems</b>	<p>Includes procurement of any kind of software oriented to medical care:</p> <ul style="list-style-type: none"> <li>- Hospital Information Systems &amp; Electronic Medical Record (HIS-EMR),</li> <li>- Laboratory Information System (LIS),</li> <li>- Radiology Information System, Picture Archiving and Communication System (RIS-PACS),</li> <li>- Pharmacy,</li> <li>- Drug Databases,</li> <li>- Care Management,</li> <li>- Diet Software,</li> <li>- Computer Physician Order Entry (CPOE),</li> <li>- Big Data analysis, etc.</li> </ul> <p>CIS <b>must be located</b> 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.</p>
<b>Medical devices</b>	<p>Any piece of hardware 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, etc.</p> <p>Includes patient implantable devices<sup>9</sup> (holters, pacemakers, insulin pumps, cochlear implants, brain stimulators, cardiac defibrillators, gastric stimulators, etc.<sup>10</sup>) or wearables (external EKG or pressure holters, glucose monitors, etc.) given they communicate by electronic means with the IT systems of the hospital.</p>
<b>Network equipment</b>	<p>Network lines (coaxial, optical), gateways, routers, switches, firewalls, VPNs, IPS, IDS, etc.</p>
<b>Remote care systems</b>	<p>Facilities or devices to provide care outside the hospital environment, especially what today is called “Hospital-based home care services”.</p> <p>Can include the remote communication “press-for-help” devices used for the help of the elderly population that live alone at home.</p>
<b>Mobile client devices</b>	<p>All piece of software that provides health assistance or medical data collection not directly connected to the hospital network; for example: telemedicine apps. It does not include health wearables as they are included into a separate category.</p> <p>Mobile client devices need a defined protocol to connect to the hospital network.</p>
<b>Identification systems</b>	<p>Systems to uniquely identify patients or medical personnel (biometric scanners, card readers etc.) and guarantee identification and/or authorization to access the IT systems.</p>
<b>Building Management Systems</b>	<p>Any type of construction that can hold medical facilities. It includes electricity lines, water, gas, medical gases, furniture, etc. except network lines, which is included under the “network equipment” category. Building Management Systems (BMS) are included in the next procurement category as they are, mainly, control systems.</p>
<b>Industrial control systems</b>	<p>Systems that control all physical aspects of the centres such as power regulation systems, door lock systems, close circuit security systems, HVAC<sup>11</sup> systems, alarm systems, water, heating, auxiliary power units, security access, elevators, fire extinguishing, etc. Nowadays, control of all these systems is managed through</p>

<sup>9</sup> Knee or hip replacements or intraocular lens are also examples of “medical devices” as well but are out of the scope of this study. For a detailed definition of “medical device” see European Parliament and Council, ‘Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices’ (2017), <http://data.europa.eu/eli/reg/2017/745/oj>.

<sup>10</sup> Aliya Tabasum et al., ‘Cybersecurity Issues in Implanted Medical Devices’, in 2018 International Conference on Computer and Applications (ICCA) (2018 International Conference on Computer and Applications (ICCA), Beirut: IEEE, 2018), 1–9, <https://doi.org/10.1109/COMAPP.2018.8460454>.

<sup>11</sup> Heating, ventilation and air conditioning system



	software systems: Building Management Systems (BMS). BMS may be acquired separately or as part of a building renovation project,
<b>Professional services</b>	All kind of services, outsourced or not, provided by professionals or companies: medical services, transportation, accounting, engineering, IT, legal, maintenance, cleaning, catering, etc.
<b>Cloud services</b>	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.

### 2.3 RELEVANT INDUSTRY STANDARDS AND GUIDELINES

*There already exist a number of regulations, international standards and good practices on healthcare systems, products and services that include cybersecurity baselines. Consult the mapping in this section to see if a relevant industry standard is available for the specific type of procurement you are planning/managing.*

There are several international standards and good practices in the market related with healthcare procurement. The following section lists existing standards and protocols that directly, or indirectly, have a relation to procurement.

As of today, ISO is developing more than 25 new standards in Medical Informatics, some of the most interesting being:

- **ISO/DTR 22696** Health informatics — Guidance for identification and authentication for connectable personal healthcare devices ,
- **ISO/DTR 21332** Health informatics — Cloud computing considerations for health information systems security and privacy,
- **ISO/WD 13131** Health informatics — Telehealth services — Quality planning guidelines,
- **ISO/AWI 22697** Health informatics — Application of privacy management to personal health information

In addition, a number of guidelines, standards and good practices exist at EU and Member State level. A brief overview of the relevant landscape is depicted in Figure 3.





Figure 3: Regulations, international standards and good practices on healthcare systems



The most relevant international standards which try to standardize the minimum requirements for a safe design, manufacture and risk management of various types of procurement are listed below and presented in more detail in Annex A.

**Table 2:** Mapping of standards per procurement type

Standards	Clinical Information Systems	Medical Devices	Network Equipment	Remote Care Systems	Mobile Client Devices	Identification Systems	Building Management Systems	Industrial Control Systems	Professional Services	Cloud Services
ISO 80001			X	X	X	X	X		X	
ISO 13972			X	X	X	X	X		X	
ISO 13485		X	X	X	X	X	X		X	
ISO 14971		X	X	X	X	X	X		X	
ISO / IEC 20000	X		X	X	X	X	X		X	
ISO 27000	X		X	X	X	X	X		X	
ISO 27799	X		X	X	X	X	X		X	
ISO 22857	X		X	X	X	X	X		X	
ISO 27019			X	X	X	X	X	X	X	
ISO 27017										X
IEC 62304	X		X	X	X	X	X		X	
IEC 60364-7-710			X	X	X	X	X	X	X	
ISA/IEC 62443			X	X	X	X	X	X	X	
DICOM			X	X	X	X	X		X	
HL7			X	X	X	X	X		X	
NIST-SP 800-66	X		X	X	X	X	X		X	
NIST CSF	X		X	X	X	X	X		X	
HTMs			X	X	X	X	X	X	X	

## 2.4 CYBERSECURITY CHALLENGES

*Many systems, products or services procured by hospitals introduce or are characterised by significant cybersecurity challenges. Consult this section for a list of the key relevant challenges and identify what are the major challenges associated with the specific type of procurement you are planning/managing. Work jointly with your IT, security or risk departments to identify the best ways to address the relevant challenges.*

According to the answers from the interviews with the stakeholders, the most challenging type of procurement was “Medical Devices” (100% of the answers) followed by “Industrial Control Systems” and “Clinical Information Systems”. As one interviewee pointed out, the most challenging threats are normally associated with procurements for which the IT department is not typically involved.

Other interesting challenges not included in the list but pointed out by the stakeholders were “Maintenance Services” and challenges associated with free software handed over by some medical suppliers.

Based on the feedback from the interviews with the stakeholders, several key challenges associated with procurement in healthcare organisations were identified. These challenges have been grouped based on the previously defined types of procurement.

### Clinical Information Systems

- **Component vulnerability:** Information systems in healthcare organisations are usually made of different pieces from different suppliers. Besides that, these systems interact and share files and data, so a vulnerability of one component can affect others.
- **Increasing interoperability:** Software specialization, and new trends as big data, analytics, create the need of sharing patient data between different systems. This process needs to be done in a secure way, using appropriate protocols and transmitting only the required data to only the right receiver.
- **Full continuous operation:** Healthcare organisations usually operate 24x7, and resources are scarce, so stopping a modality or even a desktop computer can impact seriously the service. When an incident is detected, it is sometimes really difficult to isolate the equipment, and thus this make propagation easier. In such cases the procurement process should require from providers contingency plans and redundancy.

### Medical devices

- **Manufacturing processes:** Although this topic has been traditionally strictly controlled by medical device suppliers, actually it is very common to have third-party suppliers of software and electronics in their supply chain. This introduces new challenges for manufacturers: they need not only to check materials, durability, or sterilization, they now have to test software and electronics to ensure they are robust and secure before putting the device into the market.
- **Rented equipment:** Especially when considering expensive healthcare equipment, it is common to rent devices that could have been previously used by other healthcare organisations, and often come with default set up. Procurement of rental services should establish measures to avoid risks of this practice.

- **Legacy devices:** Medical equipment usually is very expensive; these devices are expected to be in service for many years. Due to this long life cycle, buyers can sometimes have difficulties in getting maintenance support from manufacturers. For this reason, vulnerabilities cannot always be corrected, and thus can be exploited through cyberattacks.
- **Hidden functionalities:** Medical equipment is always complex to manage and set up. Neither doctors nor the IT department are usually trained on new equipment. The habitual action is to leave this equipment<sup>12</sup> in a standard setup, so preventing default passwords and ensure that unknown functionalities are not activated is another challenge in these environments. Devices can have operative procedures implemented (e.g. requests for date/time, communication of technical & service data to the manufacturer, requests for maintenance, automatic updates etc.) unknown to the buyer that could trigger security alerts on the IPS system of the hospital. That interconnectivity opens up an array of opportunities for malicious individuals to gain access to the organization's IT infrastructure.
- **Updates / Lifecycle management:** The most recent devices have usually the functionality of being operated remotely. This allows the providers to reduce maintenance costs and perform other operations. But these cases, if ignored or neglected, can result in back doors in the organisation because they are often set up without knowledge of the IT department.

#### Building Management Systems – Industrial Control Systems

- **IT/OT hybrid solutions:** Hybrid solutions make possible the convergence between digital and physical worlds, ranging from smart buildings to digital twins, and including for example real time location systems for patients and valuable assets, hospital laundries, pharmacy systems, or surgery blocks. Of course, this opens a new scenario for threats and risks that healthcare organisations should deal with.

#### Networking

- **Unprotected protocols:** As in other sectors, protocols have been designed with the use cases in mind but ignoring abuse cases. On the other hand, health data is very persistent: a data leakage could have permanent impact in patients. Improving the security of protocols used to exchange patient data is crucial.

#### Professional services

- **Human factors:** Users' awareness allows healthcare organisations to improve their level of protection almost exponentially. In healthcare, nonetheless, the pressure and the need of providing urgent health care sometimes makes more likely for a user to relax good practices in cybersecurity to provide health care to patients<sup>13</sup>.
- **Patient safety:** In healthcare organisations there are two specific conditions that make information systems different from the rest of the IS: (1) Patient data is permanent, cannot be changed if privacy is broken (as you could do with your credit card number for example); and (2) cyberattacks can become physical and cost human lives. Clinicians work hard to improve patient safety and medical devices and IT services must be considered another layer in patient safety<sup>14</sup>. This should be the key in the procurement phase specific cybersecurity requirements.

<sup>12</sup> Clemens Scott Kruse et al., 'Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends', *Technology and Health Care* 25, no. 1 (21 February 2017): 1–10, <https://doi.org/10.3233/THC-161263>.

<sup>13</sup> Ross Koppel et al., 'Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?', *Studies in Health Technology and Informatics* 208 (2015): 215–20.

<sup>14</sup> ECRI Institute, '2019 Top 10 Health Technology Hazards Executive Brief' (ECRI Institute, 2018).

# 3. CYBERSECURITY IN PROCUREMENT

## 3.1 THREAT TAXONOMY

*Different types of procurement are associated with various threats to a hospital's ICT environment. Consult the threat taxonomy presented in this section together with your IT, security or risk department to identify which threats are most relevant to your organisation. This activity should be part of the IT tasks in the hospital regardless of the procurement potential. You can then prioritise the good procurement practices presented in Chapter 4 that can mitigate the identified threats.*

Threat sources are the other risk factors that must be taken into consideration when analysing risk. A threat source is characterized as: (i) the intent and method targeted at the exploitation of a vulnerability; or (ii) a situation and method that may accidentally exploit a vulnerability<sup>15</sup>. Some examples of threat sources are: an individual, an organization, a customer, hack activist, a user, a privileged user/administrator, failure of a storage device, failure of a temperature control, failure of an operating system, fire. Keep in mind that the list of threat sources is quite large. Previously referenced NIST Special Publication 800-30 Guide for Conducting Risk Assessments appendix D, contains table D-2 with a useful taxonomy of threat sources.

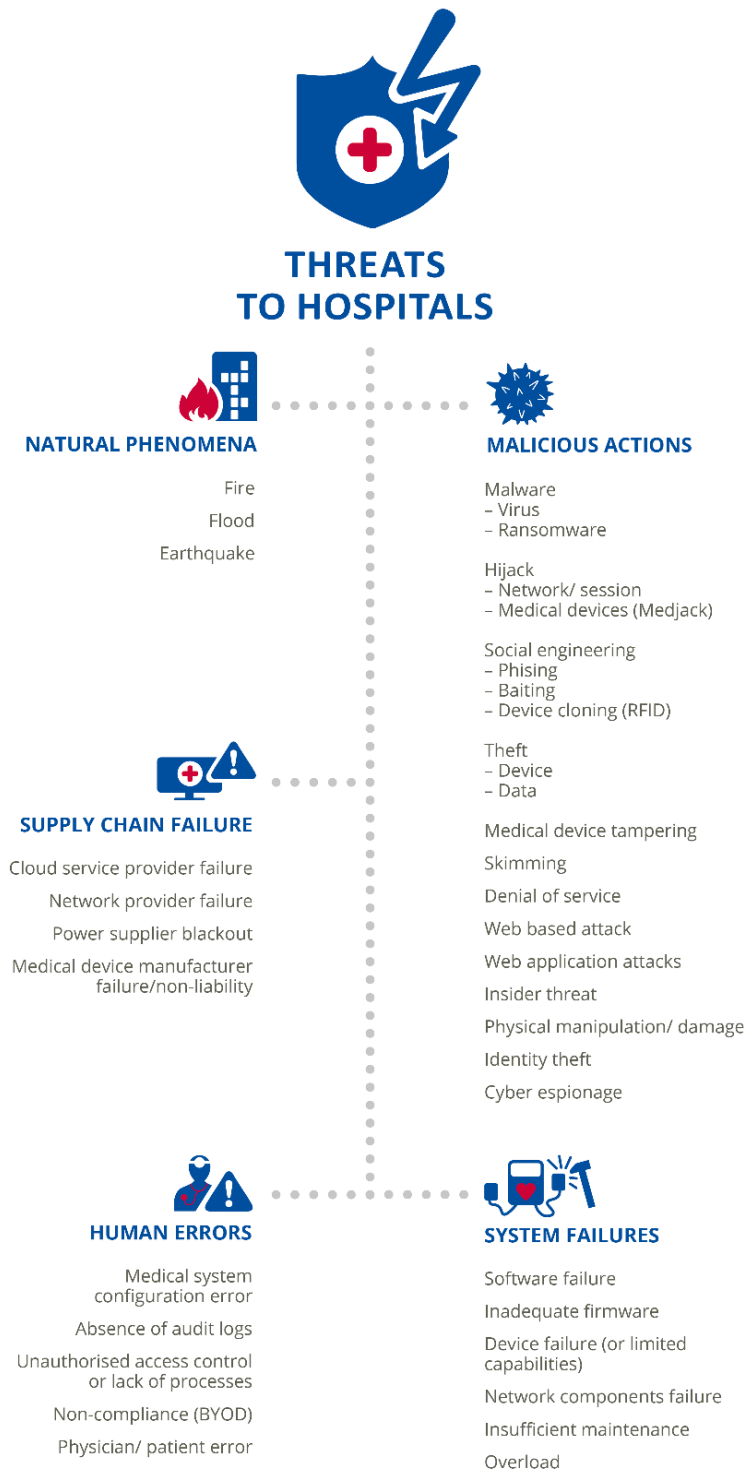
Based on the last ENISA reports on Smart Hospitals (2016)<sup>16</sup> and the 2018 threat landscape report<sup>17</sup> this study analyses the top cyber threats with a specific focus in healthcare ( for example medjacking and medical equipment threats).

<sup>15</sup> Joint Task Force Transformation Initiative, 'Guide for Conducting Risk Assessments' (Gaithersburg, MD: National Institute of Standards and Technology, 2012), <https://doi.org/10.6028/NIST.SP.800-30r1>.

<sup>16</sup> <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals>

<sup>17</sup> European Union and Agency for Network and Information Security, ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends., 2019, [https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at\\_download/fullReport](https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport).

Figure 4: General overview of healthcare threats



The proposed threat taxonomy comprises of five groups, described in more detail in the following matrices:

### 3.1.1 Natural phenomena

Threat	Description
<b>Natural phenomena</b>	<p>Fire, floods or earthquakes are infrequent but possible threats for the infrastructure and overall equipment (devices, network components etc.). Habitually, computerized tomography scan machines, magnetic resonance imaging equipment, radiotherapy equipment and other highly expensive devices are usually located in the ground floor or at the basement of the hospitals -either by regulatory laws or just because their weight and dimensions- and are specially affected by this type of phenomena.</p> <p>It should be noted, that failures due to floods or fires i.e. broken pipe flooding the basement of a patient room can have different impact than a disaster due to natural phenomena (wildfire, storm, tsunami etc.) and eventually could affect the whole hospital and its surrounding or supply chain provider.</p>

### 3.1.2 Supply chain failure

Threat	Description
<b>Cloud Services provider failure</b>	Not all services are hosted in hospital servers. Accounting, salaries, stock control may be outsourced and depend on third party cloud services. Nearly all of the personal IoT medical devices work in the cloud. In fact, some hospitals -especially regional or small associated centres-, can have their entire electronic health record system located in other site. These services, if not adequately backed up to work off-line, may cause severe disruptions in the provision of medical services.
<b>Network provider failure</b>	A network failure can have devastating effects. Most of the main hospital centres form a hub between the main building and its associated centres -mostly radiology or ambulatory or day-care centres-. Redundancy and topology design are crucial when mitigating this type of threat.
<b>Power supply failure</b>	Loss of electricity can be of importance depending of the equipment affected. Intensive care units, operative rooms, servers and clients are usually protected by uninterruptible power sources or batteries but other equipment such as MRI or CT machines can be compromised.
<b>Medical device manufacturer failure / non-liability</b>	All medical devices can have design errors in their systems. These latent errors may arise under certain circumstances during the normal use of the device. Most of the times, these errors are known and cannot be mitigated because the device does not allow for updates. If the manufacturers who make this equipment are acquired by larger companies or run out of business there may be problems with device updates or repairs. Also, security information shared with third parties can be compromised.

### 3.1.3 Human errors

Threat	Description
<b>Medical system configuration error</b>	Not changing factory-default passwords is one of the most common errors that gives attackers access to the devices once they have gained access to the network. Other errors of this kind can be, for example, to configure our device to allow incoming connections from any address or communicate using non-encrypted protocols.
<b>Absence of audit logs</b>	<p>Logs are a crucial part of the secure-test-analyse-improve strategy of security. If we assume that sooner or later our system will be compromised, logs are one of the most useful tools that we can use to trace back how attackers gained access to our system. We can also evaluate how much information was compromised. Keeping the logs secure is one of the most important tasks of security, although its absence does not compromise already implemented security.</p> <p>In some circumstances logs may be a legal requirement for normal operation of the system (e.g. access to medical history)</p>
<b>Unauthorised access control / lack or processes</b>	Due to the variety of roles in a hospital (i.e. physicians, caregivers, administration) access control procedures should be in place. As the priority to all hospital staff is care, workarounds are often the case when it comes to access control (including all types of access control from buildings to systems and accounts). This poses great threats to the hospital interconnected environment.



Threat	Description
<b>Non-compliance (BYOD)</b>	Today's employees want the freedom to work from any location and any device at any time of day. These individuals are increasingly using their personal mobile devices to undertake work tasks. From a business perspective, enabling BYOD is an advantageous strategy <sup>18</sup> . However, bring-your-own-device (BYOD) can also represent a significant risk for organisations. For the IT department, there is massive pressure to find a way to securely enable BYOD. Failure to do so can lead to malware outbreaks, noncompliance with regulatory requirements, and corporate exposure in the wake of personal device theft.
<b>Medical staff / patient error</b>	<p>There is always the possibility of human error when entering data by either part, particularly when entering the clinical history number. Sometimes two patients can have identical names and the clinical information of one can be written on the medical history of the other. This is of critical importance when the information provided will activate subsequent clinical decisions that will affect the patient's health: e.g. a patient with the same name as other could be misdiagnosed of cancer. In the worst case the patient could receive non-needed surgery (amputations) or radio/chemotherapy. On the contrary, a patient with cancer could receive an invalid report of normality and delay a treatment that could potentially improve his/her status.</p> <p>Although the impact is low because only affects one or two patients, global impact on the company's or healthcare organisation's reputation can be very high.</p>

### 3.1.4 Malicious actions

Threat	Description
<b>Malware:</b> <b>-Virus</b> <b>-Ransomware</b> <b>-BYOD</b>	<p>In healthcare organisations, IT systems are strongly interconnected and difficult to isolate without generating service disruption, creating a comfortable ecosystem for malware.</p> <p>Enterprises with a very large number of devices may have difficulties updating their licenses because of the elevated costs.</p> <p>Adware is one of the easiest ways to distribute malware and more often ignored by users<sup>19</sup>.</p> <p>Ransomware is perhaps the most known threat for healthcare organisations, due mainly to the Wannacry case. Ransomware usually makes indiscriminate low-cost attacks. It's very easy to infect healthcare infrastructure because of two factors; (i) software infrastructure is hard to keep updated because it's very difficult to get a downtime slot, (ii) machines that run legacy software that only works on specific OS or drivers' version turns out to be an easy target for these attacks. Many of these legacy devices that cannot be updated act as reservoirs for the malware helping it spread through the network.</p> <p>Enterprises that allow bring-your-own-device (BYOD) without appropriate policies are exposed to additional risks.</p>
<b>Hijack: Cryptojacking / Medjacking</b>	<p>Medical equipment needs usually real time communications, and clinicians need also a quick response from the system when they look for patient data or test information. Dedicating processor time or communication capacity to mining cryptocurrency impacts performance and of course, the health care provision.</p> <p>The difference between cryptojacking and medjacking is basically the kind of hardware involved. In the first case we are talking about general purpose IT infrastructure and in the second we are referring to IT-based medical equipment.</p>
<b>Social engineering:</b> <b>-Phishing</b> <b>-Baiting</b> <b>-Device cloning</b>	<p>Compromised email (phishing, spam and spear-phishing) is the dominating attack vector for malware infections. According to Verizon DBIR334, email compromise was the attack vector for 92.4% of detected malware<sup>20</sup>. Most organizations still allow access to private mail web accounts in most of the computers of the hospital.</p> <p>Mail addresses from clinicians are easy to collect through hospital public directories, existing presentations on the web, etc. In our research, we found both cases of using professional e-mail accounts for personal matters, and cases of using personal e-mail accounts for professional matters.</p> <p>Fight against phishing is not easy: keeping an adequate user awareness is very difficult. Multiple factors have been blamed: most personnel in the health field has no technical knowledge at all, a stressful</p>

<sup>18</sup> BYOD and GDPR: Managing the compliance conundrum. At PrivSec Report, 11<sup>th</sup> January 2019.

<sup>19</sup> ENISA Threat Landscape Report 2018. January 2019.

<sup>20</sup> ENISA Threat Landscape Report 2018. January 2019.



	<p>environment with high pressure, shift work<sup>21</sup>, staff rotation, and a lack of understanding between IT team and clinicians<sup>22 23</sup>.</p> <p>Device cloning (ID cards) requires a high level of specialization and the necessity to get closer to the victim to clone his/her ID. Two factor identification has made this type of threat very unlikely.</p>
<p><b>Theft:</b></p> <p>- Device</p> <p>- Data</p>	<p>The cost of medical devices is very high. Stealing of medical equipment is a very common crime. Devices are usually sold in the second-hand market of underdeveloped countries or for veterinary uses for a fraction of their price. Small to medium-sized portable devices as ultrasound equipment, EKG, defibrillators, infusion pumps or vital signs monitors are among the most robbed pieces.</p> <p>Devices should not expose medical data unless adequately logged in. Unfortunately, most of them use the factory default credentials.</p> <p>The lack of involvement of IT security department in setting up and managing medical equipment, the lack of risk-awareness of the staff can generate information leaks that could impact on reputation, patient privacy, penalties, or even patient safety.</p>
<b>Medical device tampering</b>	<p>Unprotected communications between medical devices and servers can result in tampering of the information. Sophisticated man-in-the-middle (MITM) attacks can change the data coming from vital signs monitors, laboratory, pathology reports or even DICOM images coming from CT scans, MRI or ultrasound systems in their way to the PACS server.</p>
<b>Skimming</b>	<p>Skimming (stealing of credit card information) can occur from breaches in patients' administrative data. It is unlikely to occur in public health systems where no payment is the rule and social security numbers are used instead. That is not the case in private institutions.</p> <p>When protection of administrative data becomes secondary against protection of medical records, a breach can occur more easily.</p> <p>Large shopping areas, and e-commerce systems seem to be the target for this type of organized criminals. Great effort from some public and private organizations has been made in the last years to prevent fraud in this area and is out of the scope of this report.</p>
<b>Denial of service</b>	<p>Denial of Service is a very common cyberattack that can take down servers at a healthcare organisation, especially because they are usually reluctant to use public cloud infrastructure, so the capacity of servers is limited. The impact can be high, depending on the type of systems affected.</p>
<b>Web based attacks</b>	<p>Extended use of undocumented web services for interoperability purposes, and the delay in applying updates, trying to keep the system configuration without changes and to reduce the downtime as much as possible, makes it easier to exploit known vulnerabilities.</p>
<b>Web application attacks</b>	<p>SQL Injection and Denial of Service represent the 68,8% of web application attacks, while in government institutions represent only the 26% or 27,7% globally. SQL injection alone represents the 46% in the case of healthcare, similar percentage to energy and manufacturing companies, another environment where industrial equipment is very frequent<sup>24</sup>.</p>
<b>Insider threat</b>	<p>Hospital staff can act as insider threats, at any position (physicians, nurses, administrative, maintenance, etc.), but patients or guests can act also from within the hospital, given that access cannot be restricted to certain areas.</p>
<b>Physical manipulation / damage</b>	<p>Medical equipment can be very expensive, and many times, physical access is granted to non-authorized or poorly trained personnel -if not-trained at all-, allowing manipulation, damages, theft or loss of this equipment or the information assets they contain.</p>
<b>Identity theft</b>	<p>There are 2 cases: employees' identity or patients' identity. The first case can be dangerous because impersonating a doctor or nurse allows, for example, to do wrong prescriptions or diagnose a patient of a certain disease, and the second case could be used to fraud the healthcare system and introduce wrong diagnoses as well.</p>
<b>Cyber espionage</b>	<p>Interest of multinational pharmaceutical industries or other interest groups on clinical research results or patient data can be one the drivers of this kind of threats. Cases have been documented of new technology that it's being tested in a hospital and other nations have been spying with the intention of copying this new technology or treatment.</p>

<sup>21</sup> Annalena Welp et al., 'Teamwork and Clinician Burnout in Swiss Intensive Care: The Predictive Role of Workload, and Demographic and Unit Characteristics', *Swiss Medical Weekly*, 24 March 2019, <https://doi.org/10.4414/smw.2019.20033>.

<sup>22</sup> Koppel et al., 'Workarounds to Computer Access in Healthcare Organizations'.

<sup>23</sup> Sean W Smith and Ross Koppel, 'Healthcare Information Technology's Relativity Problems: A Typology of How Patients' Physical Reality, Clinicians' Mental Models, and Healthcare Information Technology Differ', *Journal of the American Medical Informatics Association* 21, no. 1 (January 2014): 117–31, <https://doi.org/10.1136/amiajnl-2012-001419>.

<sup>24</sup> Positive Technologies, 'Web Application Attack Statistics: Q2 2017', September 2017, <http://blog.ptsecurity.com/2017/09/web-application-attack-statistics-q2.html>.



Threat	Description
<b>Components mechanical disruption</b>	Imaging devices such as MRI machines and CT scanners, include mechanical components which are remotely controlled. A compromise can transfer control to a malicious actor and they can cause undesired movement of these components. This can have direct impact to the patient.

### 3.1.5 System failures

Threat	Description
<b>Software failure</b>	<p>Any piece of software can have errors. Special security measures are taken in devices such as infusion pumps, electrosurgical units, ventilators, medical use lasers, or devices that use ionizing radiation to work - radiology and radiotherapy equipment- that could generate physical damage if an error occurred. Lessons have been learned from severe incidents occurred in the past<sup>25</sup>. The general rule is: all measures have to be taken so no overdose can be administered under any circumstance.</p> <p>These devices undergo extensive tests before going out to the market. In few occasions, their software is updated by the manufacturer.</p> <p>Servers are more prone to failure, not only because of failures in the design of their dedicated software but because they rely in other software platforms (operating systems, programming frameworks, databases) that can fail as well. In fact, experience has shown us that many errors occur after a software update.</p> <p>Failures in medical servers occur normally as latent errors and, in some occasions, can stop the service. They habitually disappear after server reboot. Analysis of the generated logs is crucial to find what the cause of the error was. Failures that do not cause server breakdowns or service disruption (loss of patients' appointments or patient's clinical information, for example) are usually detected several months after the system has been running.</p> <p>Several specially prepared tests should be run to ensure that the system does what it is expected to do. As these systems run 24-7, finding downtime slots to run the tests can be very difficult if not impossible.</p> <p>Frequent server failures deteriorate medical care and degrade confidence in the institution.</p>
<b>Outdated firmware</b>	Lack of procedures in place to update firmware in all devices (medical or not) in the hospital, is a top threat for healthcare organisations and namely hospitals. Legacy systems and software offer back doors to malicious actors that can access sensitive healthcare data.
<b>Device failure</b>	Failure of simply limited/reduced capability may severely impact processes that rely, e.g. on the real-time collection of patient data, such as glucose measuring devices;
<b>Network components failure</b>	The interconnected ecosystem of a hospital has to be resilient as the requirement for real time data analysis is high. If a component fails this can cause unavailability of a system, which can have cascading effects to other healthcare systems (i.e. Patient Health Record)
<b>Insufficient maintenance</b>	Lack of updates or lack of patching is another very common threat that can have great impact to the healthcare organisation, i.e. malware spread. Operational issues might be left unresolved eventually jeopardising patients' health.

<sup>25</sup> More information at ["Overview of some major incidents in radiotherapy and their consequences"](#), Hamish Porter. British Institute of Radiology. September 2012.



### 3.2 RISKS IN PROCUREMENT

*Each type of procurement carries its own risk factors. Consult the following list to identify the main risks associated with the specific type of procurement you are planning/managing. Work jointly with your IT, security or risk departments to identify the best ways to address the relevant risks.*

Each type of procurement carries its own risk factors. It is important that administrators of healthcare organisations understand these risk factors and the negative impact they could cause on the IT infrastructure, patients’ health, patients’ information, diagnosis and quality of service.

The following table illustrates some indicative risk factors associated with each type of procurement. This is not a comprehensive list of risk factors and the list should not be considered exhaustive. Next to each factor there are sample negative outcomes.

**Table 3: Risks in procurement**

Type of procurement	Risk Factors	Negative outcome
<b>Clinical information systems</b>	Infrastructure incapable of handling system	New system sluggishness due to under rated server CPU or small system memory. Disk errors due to not enough disk space. Network bandwidth unable to handle data traffic, affecting all the Organization’s network communications.
	Poorly designed or poorly programmed system	Erroneous results due to poor programming. System errors due to lack of input validations. Long user learning curve due to poorly designed user interfaces. User errors due to poorly designed user interfaces.
	Lack of security considerations	Stolen credentials due to poor handling of passwords, i.e., passwords stored in clear text, allows intruder to steal patients’ data. Fraud and errors, due to absence of separation of duties. Opportunity for attackers due to lack of input validations, i.e., SQL injection. Absence of transaction records (logging) allows attacked to hide their actions.
<b>Industrial Control Systems</b>	Known (published) service password	Attackers are able to control BMS devices due to known (published) administrator’s login credentials not changed during installation. Once the attacker controls the device, he/she utilizes the device to launch Denial of Service attacks on the Organization’s infrastructure.
	Use of insecure network protocols	Due to the use of insecure network protocols (HTTP), attackers are able enter the Organization’s network.
	BMS installed with open and exposed ports	Open ports on a device can be used as an attack vector.
	Poor physical security protection of BMS devices controllers and workstations.	Attackers may gain physical access to consoles to install malware or to sabotage the devices.
<b>Medical Devices</b>	Absence of authentication controls	Intruder manages device console to produce erroneous results.



	Unencrypted data	Transmission of data in clear text, allows attackers to alter sensor's results.
	Use of insecure network protocols	Attackers enter the Organization's network.
<b>Mobile connected medical devices</b>	Use of vulnerable smartphone	Attackers may interfere with the correct operation of the medical device.
<b>Identification systems</b>	Unencrypted data	Due to the clear text transmission, attackers are able access user identification and gain access to facilities.
<b>Cloud services</b>	Improper implementation	Confidential information made public due to poor security measures on the client side. System unavailable due to Denial of Service attacks.

# 4. GOOD PRACTICES FOR CYBERSECURITY IN PROCUREMENT

*How to use the good practices of this chapter:*

**Step 1:** *Identify the type of procurement you are planning/managing (Ch.2)*

**Step 2:** *(Optional) Identify the threats you are most interested in mitigating (Ch.3)*

**Step 3:** *Identify the good procurement practices relevant for the identified type of procurement (and threats)*

**Step 4:** *Assess on which phase of the procurement lifecycle cybersecurity should be addressed. Understand the description and objectives to be achieved in the selected good practices in the corresponding phase.*

**Step 5:** *Using the graphs provided, understand in which procurement phases each good practice can be implemented*

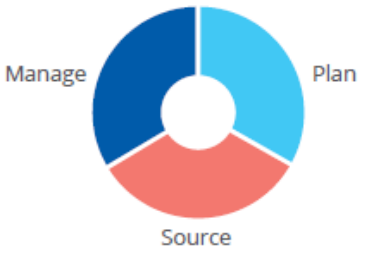
**Step 6:** *See the indicative examples of how to implement each practice or evidence that can be requested from supplier; adapt to your own procurement practices/methodology as needed.*

This chapter presents good practices for enhancing cybersecurity in procurement. The good practices categorised per phase of the procurement lifecycle and for each one of these description, examples, procurement type addressed, mitigated threat and evidence are included. The general practices apply to all three stages of the lifecycle. In some cases, a good practice may apply to two phases, in which case they are categorised under the phase where they should first be applied or where they are most relevant.

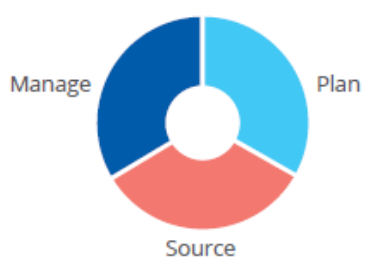
The list of good practices below is by no means exhaustive; it gives however a solid advantage to the healthcare IT professional responsible for purchasing equipment in a hospital. The set of good practices are the collective result of all input received by healthcare professionals interviewed. The reader can adapt the list based on the priorities of his/her organization.

## 4.1 GENERAL GOOD PRACTICES

### GP 1. Involve the IT department in procurement

	<p>Involve the IT department in the different stages of procurement to ensure that expertise in cybersecurity aspects is considered</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Involve IT staff in drafting cybersecurity requirements</li> <li>• Consult IT department to integrate cybersecurity considerations when planning new procurements</li> <li>• Make cybersecurity requirements part of the RfP</li> <li>• It should be part of healthcare organization's procurement policy to include IT departments in all system, service or device acquisitions committees</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>All</p>
<p><b>Related Threats</b></p>	<p>All</p>

### GP 2. Implement a vulnerability identification and management process

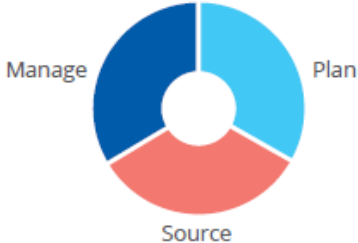
	<p>Ensure that vulnerabilities are considered before procuring new products or services and that vulnerabilities of existing products/services are monitored throughout their lifecycle</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Establish a vulnerability management process to monitor and address vulnerabilities of ICT products/services</li> <li>• Information on existing vulnerabilities may be obtained from the manufacturer or from public sources, such as the NIST vulnerability database<sup>26</sup></li> <li>• Address newly identified vulnerabilities accordingly and include provisions in the RFP/contract for supplier responsibility in addressing vulnerabilities via timely patching</li> <li>• Healthcare organizations may consider including a requirement for the Bill of Materials (BOM<sup>27</sup>) used in acquired systems or products. This will help in the tracking of vulnerable systems in a healthcare organization's infrastructure based on publicly available vulnerability information.</li> </ul>

<sup>26</sup> <https://nvd.nist.gov/vuln/search>

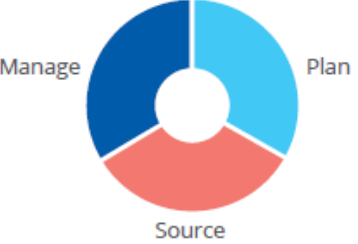
<sup>27</sup> The practice of having a vendor publish a Bill Of Materials (BOM) of the actual software and hardware used in a system allows any third party to track independently whether a certain device may be susceptible to a certain known vulnerability. It is common for such BOM information to be disclosed to the Notified Bodies, so that the Notified Bodies may disclose advisories about certain medical systems and devices. However, it may be beneficial for healthcare administrators to also have access to such information in order to track vulnerable components across their infrastructure.

<b>Related Procurement Types</b>	Clinical information systems, medical devices, networking equipment, remote care system, mobile client devices, identification systems, industrial control systems, cloud services
<b>Related Threats</b>	All

**GP 3. Develop a policy for hardware and software updates**

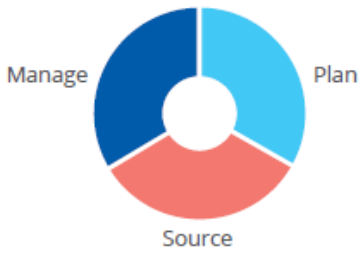
	<p>Develop an update policy to ensure that the latest patches to your OS and Software are applied and that the antivirus Software is updated.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Create a registry / IT asset inventory of all current SW and HW running including versions of SW and HW installed on them.</li> <li>• Regularly investigate if new patches are released.</li> <li>• Inform CISO/ISO of these new releases.</li> <li>• Test the proposed patch in some machines before taking the decision to patch all the machines.</li> <li>• Determine the most suitable timing to apply the patches in every segment of the network.</li> <li>• Determine workarounds for machines that cannot be patched.</li> <li>• Document the update procedure.</li> <li>• Define the involvement of third party providers.</li> <li>• Defined the actions to take to revert the situation if patched machines do not work as expected</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Medical Devices, Clinical Information Systems, Networking Equipment, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud Services</p>
<p><b>Related Threats</b></p>	<p>Malicious Actions, Supply Chain Failure, System Failures</p>

**GP 4. Enhance security controls for wireless communication**

	<p>Access to the Hospital's Wi-Fi networks should be limited and strictly controlled. Number of devices connected should be monitored and in the case of medical devices should be verified and restricted. Non authorized personnel should not have access to the Wi-Fi.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• By default, strong Wi-Fi passwords (keep log of the frequency the password is changed). This should be linked with a policy</li> <li>• Make two-factor authentication obligatory</li> </ul>

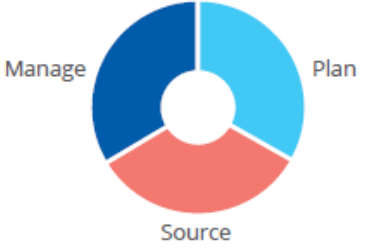
	<ul style="list-style-type: none"> <li>Medical devices that require wireless communication have a dedicated wireless network with strict access control and supporting dedicated policy</li> <li>Access from public devices is prohibited</li> </ul>
<b>Related Procurement Types</b>	Medical devices, remote client devices, identification systems, cloud services
<b>Related Threats</b>	Malicious actions, human error

**GP 5. Establish testing policies**

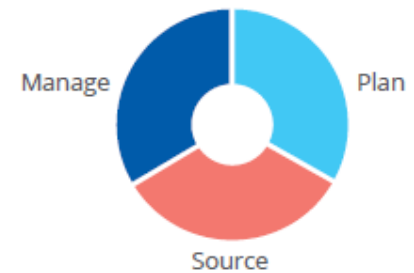
	<p>The healthcare organisation should establish a minimum set of security tests to be performed on acquired products or system, depending on the product/system type. It is also important to note that a newly acquired or newly configured product must undergo a penetration test in its actual installed environment. In the same way, remediating action taken must be inline with the operational parameters of the actual environment.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>For any type of product or system a set of security tests and assorted thresholds are defined by the healthcare organisation</li> <li>Testing policies cover all stages of procurement and may include periodic security audits and penetration tests of systems already in production environment</li> <li>Testing and thresholds are communicated to suppliers and are part of the RfP</li> <li>Acceptance criteria are defined on the basis of the security tests before the finalisation of procurement</li> <li>The RfP/contract states specific supplier responsibilities to address findings following security tests of systems in production</li> <li>All the test policies should be revised and approved by the CISO</li> <li>Some systems bill depending on the load. Talk about this issue with the provider before running load tests that could entail a cost</li> <li>Always prepare a contingency plan in case the server, the communications system or the medical device stops working during a test</li> <li>If the test load can potentially permanently stop a medical device or medical system, verify if your maintenance plan covers a reset &amp; reboot of the device/system</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Clinical information systems, medical devices, networking equipment, remote care system, mobile client devices, identification systems, building management system, industrial control systems, cloud services</p>
<p><b>Related Threats</b></p>	<p>Malicious actions, system failures, human errors</p>



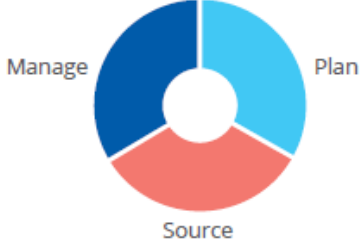
**GP 6. Establish Business Continuity plans**

	<p>Business continuity plans should be established whenever the failure of a system may disrupt the hospital's core services and the role of the supplier in such cases must be well-defined</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• It should be clear from the RFP what will be the supplier's assistance services in case of service interruption, including the cost of the supplier's services (during and after warranty) and the response time (SLA) expected</li> <li>• Different disaster scenarios must be thought out when planning for business continuity, and if the business continuity strategy includes supplier's assistance, this must be clearly stated in the RFP and put into the final contract</li> <li>• Costs and service level requirements for business continuity services must be made clear during the RFP process</li> <li>• If failure of a newly acquired system may jeopardise the hospital's ability to provide core services, the Business Continuity Plan must establish the strategy (replace the device or change faulty components), the means and the procedures necessary for an organization to keep its critical services available under the worst of circumstances</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Medical Devices, Clinical Information Systems, Networking Equipment, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud Services</p>
<p><b>Related Threats</b></p>	<p>Malicious Actions, Supply Chain Failure, System Failures</p>

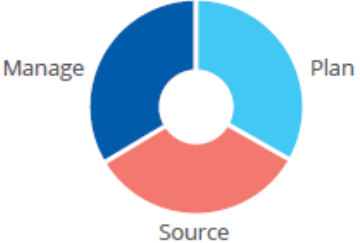
**GP 7. Take into account interoperability issues**

	<p>Interoperability is one of the greatest cybersecurity risk for healthcare organisations. The hospital's IT ecosystem is comprised by different components medical devices, networking equipment, remote care systems etc. Some of these components exist already (legacy IT) and connection with new components might result into security gaps.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• The supplier should indicate how the solution proposed is integrated to the already existing system. If necessary they should include in the offer the technical documentation explaining how integration will take place</li> <li>• The supplier should also ensure that they monitor transmission (at least for a predefined period of time) to avoid data loss</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Clinical information systems, medical devices, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud services</p>
<p><b>Related Threats</b></p>	<p>System failures, Human Error, Malicious actions</p>

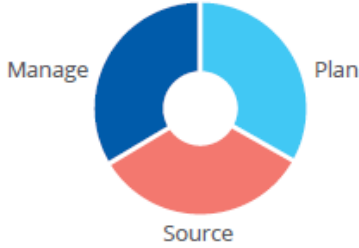
**GP 8. Enable testing of all components**

	<p>Information systems should be thoroughly tested to guarantee they deliver what is promised: verify easiness of use, check the correctness of results under load, and check for security flaws (weak password policy, SQL injection). Testing should be a requirement in procurement as well as monitoring during testing. Testing should be aligned with testing policies</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• The supplier should include testing scenarios for the devices/ systems offered. They should explain how testing should take place and how it will be coordinated. Define benchmarks for every test</li> <li>• Reports from testing could be shared in confidence</li> <li>• Always prepare a contingency plan in case the server, the communications system or the medical device stopped working during the test</li> <li>• If the test load can potentially permanently stop a medical device or medical system, verify if your maintenance plan covers a reset &amp; reboot of the device/system</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Clinical information systems, medical devices, remote client devices, identification systems, cloud services, industrial control systems, remote care system, building management system, mobile client devices</p>
<p><b>Related Threats</b></p>	<p>Malicious actions, human error, system failures, supply chain failure</p>

**GP 9. Allow auditing and logging**

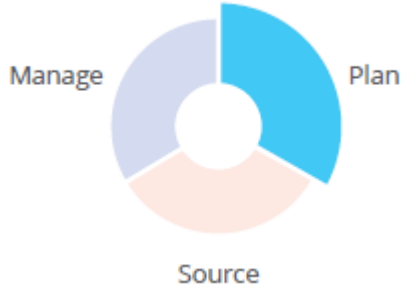
	<p>Logs are a crucial part of the secure-test-analyse-improve strategy of security. If we assume that sooner or later our system will be compromised, logs are one of the most useful tools that we can use to trace back how attackers gained access to our system. We can also evaluate how much information was compromised. Keeping the logs secure is one of the most important tasks of security, although its absence does not compromise already implemented security</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Create a secure Central Logging System to keep a copy of the logs so these files can be safely off-site in a secure location</li> <li>• Maintaining an external log system also allows for convenience. For instance, if you have a server that crashed and is unresponsive, you can check the kernel error logs on your centralized syslog server</li> <li>• The supplier could enable access to the logs for auditing purposes</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Medical Devices, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems</p>
<p><b>Related Threats</b></p>	<p>Malicious Actions, Supply Chain Failure, System Failures</p>

**GP 10. Encrypt sensitive personal data at rest and in transit**

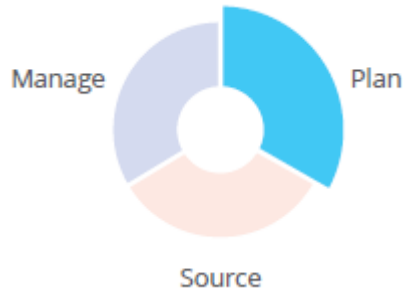
	<p>As a minimum, define a policy for systems, services or devices processing GDPR's Article 9 special categories of personal data. These types of information must be always encrypted (whenever stored or transmitted). For all other personal data categories, require encryption whenever the data leaves the Organization. Be aware that in many instances this requirement does not fall on the supplier of the system, service or device, but on the Organization itself. Data might be copied to an external disk drive for storage in an alternate site. In this case, it is the Organization's responsibility to provide the mechanism for encryption</p> <p>If data has to leave the Organization's facilities as a system-to-system communications process (sending data results to a remote processing centre), then it is the supplier's responsibility to provide a secure encrypted communications protocol</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Define if data must be encrypted, at storage or during transmission. Include this requirement in the RfP. In the offer provided by the supplier look for the algorithms and encryption methods. At this stage the Data Protection Officer should be advised.</li> <li>• The supplier should explicitly define encryption methods for data at rest, data in transit and for different types of data (sensitive health data vs personal data)</li> <li>• Sometimes the devices are unable to encrypt the information they provide. Adequate gateways for encryption should be provided between the device and our network</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Medical Devices, Clinical Information Systems, Networking Equipment, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud Services</p>
<p><b>Related Threats</b></p>	<p>Malicious Actions, Supply Chain Failure, System Failures</p>

## 4.2 PLAN PHASE PRACTICES

### GP11. Conduct a risk assessment as part of the procurement process

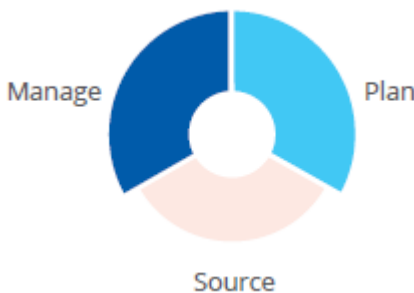
	<p>As part of the procurement process, healthcare organizations should conduct risk assessments.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Before launching a new procurement process, healthcare organisations should assess the impact of the new acquisition on their IT security risk (e.g. new risk, increase/decrease in likelihood or impact of existing risk)</li> <li>• After identifying the risks associated to the acquisition of a system, service or devices, a strategy for dealing with them must be designed and integrated in their respective procurement (including budget changes, specifications changes, etc.)</li> <li>• Risks should be identified early in the procurement process</li> <li>• Procurement planning may be cancelled or alternative solutions should be examined in case of a significant increase in IT security risk associated with a planned procurement</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>All</p>
<p><b>Related Threats</b></p>	<p>All</p>

### GP 12. Plan network, hardware and license requirements in advance

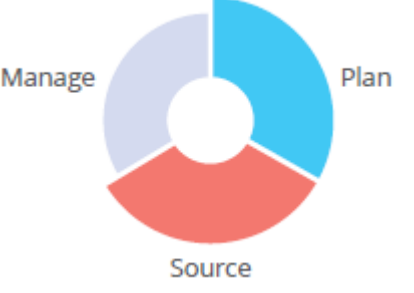
	<p>Assess whether the new systems, service or device requires third party software or whether the system will use current software but will need additional licensing. Match hardware requirements (disk space, bandwidth, CPU capacity, memory) gathered from suppliers during the RFP against current and already planned capacity usage, to determine whether additional upgrades and/or purchases must be made before installation to accommodate the new system.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Some devices come with their own free-of-license software, others need acquisition of additional software from the same company. Make your legal department verify the terms of the licenses and their scope</li> <li>• Investigate if the software can be used directly as-provided or needs to be configured</li> <li>• Check if licenses have to be renewed and if updates are covered</li> <li>• Check that you have available space in your data centre to accommodate the new servers</li> </ul>

	<ul style="list-style-type: none"> <li>Some of your external IT providers may need space in your data centre. Reserve some space for unexpected future needs (and IPS/IDS server for example)</li> <li>Ensure that your existing power system (including auxiliary power units) has enough capacity. Habitually there is lack of available plugs for the new devices</li> <li>Plan how the new devices will be physically linked to your network</li> </ul>
<b>Related Procurement Types</b>	Clinical Information Systems, Networking Equipment, Identification Systems, Industrial Control Systems.
<b>Related Threats</b>	Supply Chain Failure, System Failures, Natural Phenomena, Human errors

**GP 13. Identify threats related to procurement products or services**

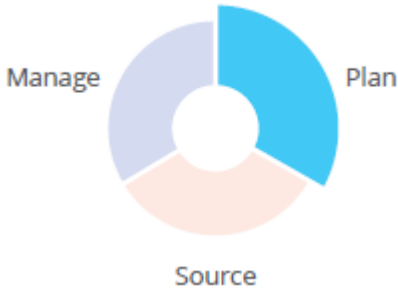
	<p>Cybersecurity threats should be considered when planning procurement of a new system, product or service and threat identification should be continuous in the procurement lifecycle</p>
<b>Examples/ Evidence</b>	<ul style="list-style-type: none"> <li>Use a structured approach to accurately identify relevant threats</li> <li>Include all relevant stakeholders when assessing threats associated with a new procurement</li> <li>The healthcare organisation's threat modelling process should be updated if applicable following the procurement of a new product or service</li> </ul>
<b>Related Procurement Types</b>	All
<b>Related Threats</b>	All

**GP 14. Segregate your network**

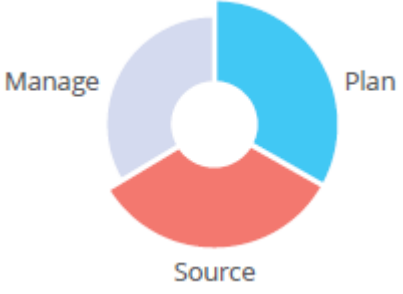
	<p>Sometimes the inherent vulnerabilities of the devices connected to the network cannot be mitigated: for example, legacy devices that use Windows NT that cannot be upgraded to newer OS. To protect the existing IT infrastructure from these devices, compensating controls must be implemented. It is important to isolate all network connected devices from the rest of the network. To do so, implement network segmentation. With network segmentation network traffic can be isolated and / or filtered to limit and / or prevent access between network zones</p>
<b>Examples/ Evidence</b>	<ul style="list-style-type: none"> <li>In the RfP the hospital should provide a rough overview of the current network topology and require the potential vendor to provide a new topology taking into account network segregation practices</li> <li>The vendor should provide information on security perimeter for the network based on the medical devices connected. This information should be included in the RfP</li> </ul>

<b>Related Procurement Types</b>	Medical Devices, Clinical Information Systems, Networking Equipment, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud Services
<b>Related Threats</b>	Malicious Actions, Supply Chain Failure, System Failures

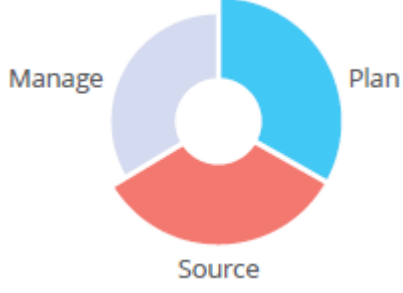
**GP 15. Determine network requirements**

	<p>After creating the network and components topology (how the devices are connected to the systems), the hospital professionals should list the security requirements for each different component also to ensure interoperability and avoid gaps (bandwidth requirements etc.). The hospital needs to know beforehand the security features they want the network equipment to have</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Check your switches. Ensure that you have available space to connect the new servers and devices</li> <li>• Create new virtual networks if needed</li> <li>• Are there enough wall-plugs or will devices communicate wirelessly?</li> <li>• Is bandwidth adequate? Verify if new lines are to be installed or if the wireless router has enough speed and capability</li> <li>• Some devices may use different protocols other than TCP/IP. Check if they will need special gateways to communicate with your network</li> <li>• Some devices do not encrypt communications by default. Check if the device has encryption capabilities or if you have to provide them by yourself through a gateway before data enters your network</li> <li>• Ensure that your device will not initiate unexpected communications with third parties</li> <li>• Do external devices need a dedicated entry gateway or firewall?</li> <li>• Check and document ports in use</li> <li>• Design a redundant topology in case of main communications line failure</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Clinical Information Systems, Networking Equipment, Identification Systems, Industrial Control Systems, Cloud Services, Remote care systems, Mobile client devices.</p>
<p><b>Related Threats</b></p>	<p>Supply Chain Failure, System Failures, Natural Phenomena</p>

**GP 16. Establish eligibility criteria for suppliers**

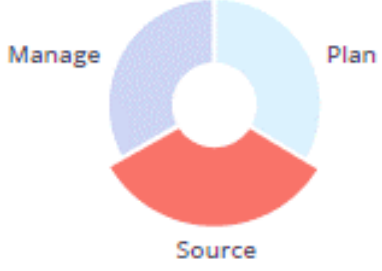
	<p>Establish security baseline requirements and translate them into eligibility criteria when selecting suppliers.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>For procurement purposes, healthcare organisations should have baselines for common components such as PCs, Operating Systems, communication protocols (e.g. no HTTP allowed), authentication mechanisms (Single Factor Authentication or Two Factor Authentication), databases, encryption, etc. Manufacturers that do not comply with the baselines, cannot participate in the procurement process</li> <li>Determine minimum security certification requirements for suppliers for different types of procurement (e.g. for the supply of security services, the supplier must be ISO 27001 certified)</li> <li>Include the security baselines as part of the RFP document (eligibility criteria)</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Medical Devices, Clinical Information Systems, Networking Equipment, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud Services</p>
<p><b>Related Threats</b></p>	<p>Malicious Actions, Supply Chain Failure, System Failures</p>

**GP 17. Create a dedicated RfP for procuring Cloud Services**

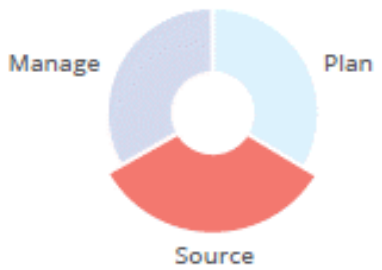
	<p>When procuring Cloud Services, especially in the case of hospitals, specific RfP should be put in place taking into account the regulatory and policy requirements. In several Member States (MS), the state has issued guidelines on what to ensure when buying cloud services</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>The Cloud service provider (CSP) should concretely state where the hospital data is stored. The hospital should demand that the sensitive data remains in the EU borders (so that EU data protection regulation applies). They should also explain which encryption mechanisms they use</li> <li>The CSP prove redundancy and business continuity in case of an incident. Also they should share the process for incident reporting (as per the requirements of the NIS Directive)</li> <li>The CSP could share results of auditing and penetration testing with the Hospital, in confidence</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Cloud services</p>
<p><b>Related Threats</b></p>	<p>Malicious Actions, Supply Chain Failure</p>

### 4.3 SOURCE PHASE PRACTICES

#### GP 18. Require cybersecurity certification

	<p>Healthcare organisations should prioritise the procurement of assets that are certified against cybersecurity schemes/standards.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Procured medical devices should adhere to the Medical Devices Regulation (procurement should require the manufacturer to provide evidence)</li> <li>• Procurement should prioritise products that have been certified against EU cybersecurity certification schemes, if applicable</li> <li>• For external services, such as cloud services, it is important to require that the provider of the service has accredited security certifications, such as ISO 27001/ ISO 27018/ CCM etc.</li> <li>• When looking at certifications, it is important to understand the scope of the certification and the scope of the service to be contracted. A provider of cloud services might be ISO 27001 certified on some parts of the service (customer support service) but not in other services which could be of more importance to the Organization</li> <li>• If available online, healthcare organisations should review the vendor certificates which come with the full report from the certification authority, detailing its findings. The scope chapter of the report typically details each service under scope. These documents are made available to provide assurance on the offered services</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Medical Devices, Clinical Information Systems, Networking Equipment, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud Services</p>
<p><b>Related Threats</b></p>	<p>Malicious Actions, Supply Chain Failure, System Failures</p>

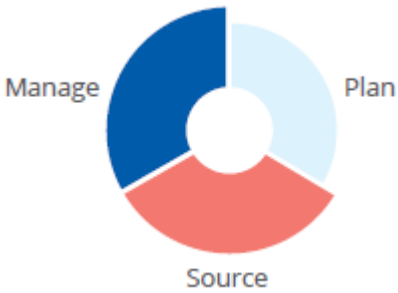
#### GP 19. Conduct data protection impact assessments for new products or services

	<p>Assess the impact on data protection issues and compliance when planning the procurement of a new system or service.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Whenever the system, device or service under consideration processes large volumes of special categories of information, a data protection impact assessment (DPIA) must be conducted</li> </ul>

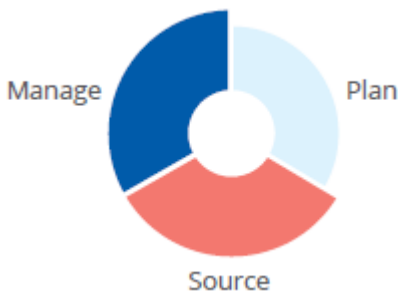


	<ul style="list-style-type: none"> <li>Document the need for any given supplier to process personal data and limit the data to whatever is necessary</li> <li>Fully document the type of data that needs to be processed by a new product/system and apply limitations in the RFP requirements</li> </ul>
<b>Related Procurement Types</b>	Clinical information systems, medical devices, networking equipment, remote care system, mobile client devices, identification systems, professional services, cloud services
<b>Related Threats</b>	Malicious actions, human errors

**GP 20. Set gateways to keep legacy systems/machines connected**

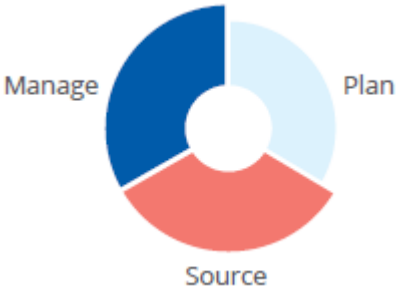
	<p>Whenever a medical device must use an old version of OS known to have vulnerabilities it should be maintained off the network; instead, a PC gateway should be developed to communicate with this device to obtain the data and pass it to the network, implementing encryption.</p> <p>Sometimes a whole segment of the network should communicate through this gateway. (e.g. all laboratory equipment). This gateway provides excellent frontier control in case of problems inside these groups. Blocking the gateway isolates all machines upstream. Follow this recommendation whenever the machines inside the segment do not need to communicate with the rest of the network except for one or two CIS servers.</p>
<b>Examples/ Evidence</b>	<ul style="list-style-type: none"> <li>Due to hardware or other requirements, some medical devices do not allow for updates (e.g. some ultrasound machines may run on old versions of Windows)</li> <li>Medical devices have a long lifespan. The drivers used to communicate with the machine may not be available in newer versions of the OS and old OS versions must be kept to access data in the machine</li> <li>Community or Day Care centres may be using devices that were discarded for use in the hospital but are still useful for not-so-demanding environments as these kind of centres</li> </ul>
<b>Related Procurement Types</b>	Medical Devices, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems
<b>Related Threats</b>	Malicious Actions, Supply Chain Failure, System Failures

**GP 21. Provide cybersecurity training on the organization's security practices to staff and external consultants**

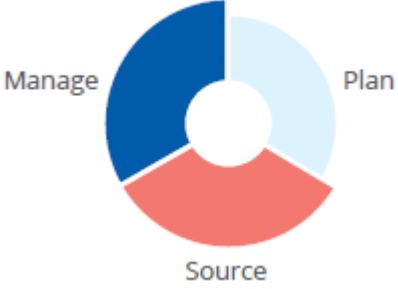
	<p>Ensure that internal staff or external contractors/consultants working on premise are adequately trained in the healthcare organisation's security practices.</p>
---	--

<b>Examples/ Evidence</b>	<ul style="list-style-type: none"> <li>• Technical staff receive periodic security training in relation to the systems they operate or maintain</li> <li>• Technical staff receive specific ad hoc security training when they need to operate or maintain a newly procured product</li> <li>• General staff (physicians, nursing staff etc) should undergo a training on the organisations information security policy and procedures.</li> <li>• External contractors/consultants that are contracted to work on premise undergo mandatory training in the healthcare organisation's security policy and security practices related to their function</li> </ul>
<b>Related Procurement Types</b>	All
<b>Related Threats</b>	Malicious actions, human errors

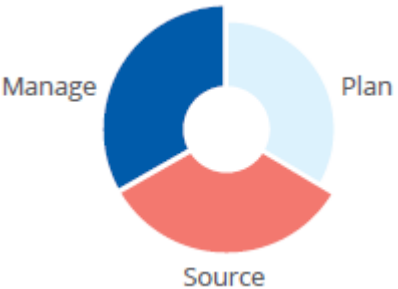
**GP 22. Develop incident response plans**

	<p>Develop incident response plans that cover newly acquired products or systems.</p>
<b>Examples/ Evidence</b>	<ul style="list-style-type: none"> <li>• Develop a response plan setting out what the organisation's staff should do in the event of a cybersecurity incident and establish the respective roles and responsibilities</li> <li>• Ensure critical updates are implemented, including applying software patches and keeping anti-virus software up to date</li> <li>• Determine appropriate communications channels in case of an incident, including between the hospital and the supplier</li> <li>• Conduct periodic tests of the incident response plans for all products/systems and conduct at least one incident response plan test for newly acquired products/systems</li> </ul>
<b>Related Procurement Types</b>	Medical Devices, Clinical Information Systems, Networking Equipment, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud Services
<b>Related Threats</b>	Malicious Actions, Supply Chain Failure, System Failures

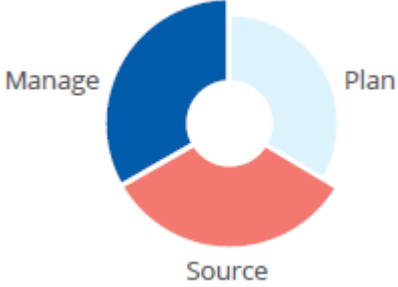
**GP 23. Involve vendor/manufacturer in incident management**

	<p>Systems and devices eventually fail, due to inaccurate coding, improper handling, or just tear and wear. It should be clear from the RfP what will be the supplier's assistance services in these eventualities, the cost of its services (first year and years after) and the response time (SLA) expected.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• The supplier should include in the offer the details of his role when handling an incident (depending on whose liability it is)</li> <li>• The supplier should include in the offer the cases under which he needs to report to the hospital, taking into account regulatory obligations</li> <li>• Engagement of other national bodies i.e. sector specific national CSIRT should be described and formalised</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Medical Devices, Clinical Information Systems, Networking Equipment, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud Services</p>
<p><b>Related Threats</b></p>	<p>Malicious Actions, Supply Chain Failure, System Failures</p>

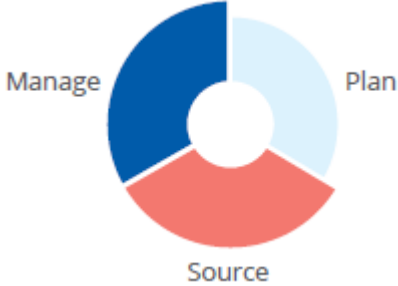
**GP 24. Schedule and monitor maintenance operations for all equipment**

	<p>Following the HW and SW update policy, maintenance operations should take place for all different types of equipment including the ones that comprise the building management system. Maintenance should make ensure an adequate level of functionality of the equipment and decide for any updates/patches etc.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Indicative maintenance schedule should be included in the proposal from the supplier. The role of the hospital IT professional should be described (monitoring the operation)</li> <li>• Maintenance logs</li> <li>• If the maintenance operation reveals a need to patch or update then another procedure should be triggered</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Clinical Information Systems, Networking Equipment, Medical Devices, Building management systems, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud Services</p>
<p><b>Related Threats</b></p>	<p>Human Error, System Failure, Natural disaster</p>

**GP 25. Remote access should be minimised and administered**

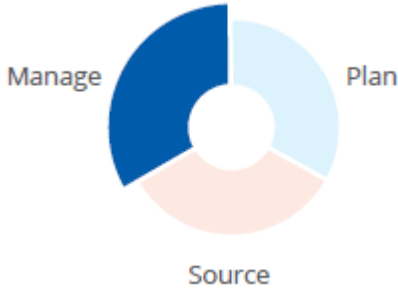
	<p>Every supplier should have a defined protocol to access the hospital network. Access should be predefined, approved and monitored. In case of an emergency situation, specific alert should be raised. Policies should include when and how the provider can access the device. Remote access should be for maintenance purposes only. No personal data should be obtained during this process. The information that can go out of the system and be processed by the supplier should be clearly defined in the contract.</p> <p>Routers and gateways should be configured in a way that external communications with the supplier should be limited to the device they have to control only.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Check configuration files for all network components and medical devices</li> <li>• Enable 2 factor authentication of remote access to PET/CAT scanners and MRI machines</li> <li>• Enable remote access only through VPN</li> <li>• Enforce access control: supplier should have access only in the device they provided and in pre-arranged time intervals</li> <li>• These clauses should be explained in the vendor proposal</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Medical Devices, Clinical Information Systems, Networking Equipment, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud Services</p>
<p><b>Related Threats</b></p>	<p>Malicious Actions, Supply Chain Failure, System Failures, Human Error</p>

**GP 26. Require patching for all components**

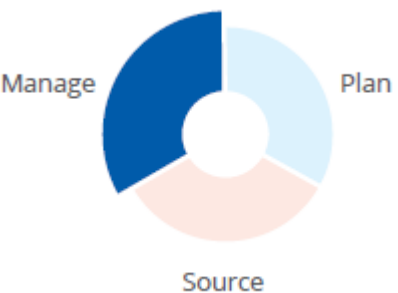
	<p>Patching is a basic requirement the hospital will set to the supplier. Patching cannot take place at any time interval, however there is a procedure to be followed. Information for patching should be included in the RFP.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• The supplier in the offer should explain the procedure for patching. The supplier should also include the role of the hospital IT professionals in this process. The process should be explicit for each component</li> <li>• The supplier should present also a redundancy plan in case the patch did not function as expected, roll back procedure needs to be in place</li> <li>• A test of the proposed patch in some machines before taking the decision to patch all the machines. Results of the test should be provided to the hospital IT professionals</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Medical Devices, Clinical Information Systems, Networking Equipment, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud Services</p>
<p><b>Related Threats</b></p>	<p>Malicious Actions, Supply Chain Failure, System Failures</p>

#### 4.4 MANAGE PHASE PRACTICES

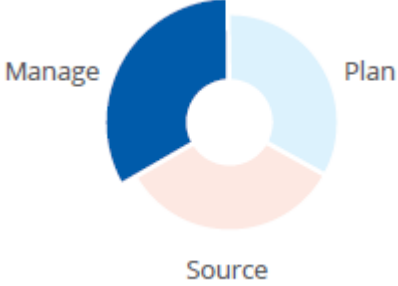
##### GP 27. Raise cybersecurity awareness among staff

	<p>Ensure staff is aware of cybersecurity risks associated with newly acquired products or services.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Adapt periodic or ad hoc awareness raising campaigns to include newly procured products or services</li> <li>• Conduct awareness campaigns for risks associated with newly procured products or services</li> <li>• Conduct specific awareness campaigns for good cyber hygiene practices when newly procured products or services introduce changes in the daily working methods of clinical staff (e.g. migration of services to the cloud or digitalisation of processes)</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>All</p>
<p><b>Related Threats</b></p>	<p>All</p>

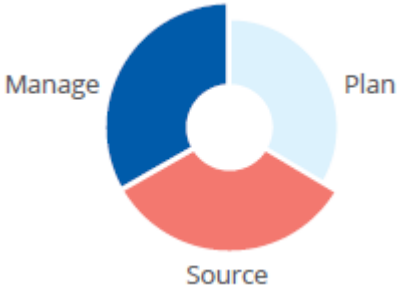
##### GP 28. Perform asset inventory and configuration management

	<p>Ensure that the IT inventory is appropriately updated when any component is added or removed from the ICT environment and that baseline security configurations for ICT components exist and are managed appropriately.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Ensure that an IT asset inventory management process is in place and that the IT asset inventory is updated when a new component is added, modified or removed</li> <li>• Ensure that baseline security configurations for IT component exist and are updated accordingly</li> <li>• Create baseline security configurations for any new type of product/system that is acquired before it is deployed in a production environment</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Clinical information systems, medical devices, networking equipment, remote care system, mobile client devices, identification systems</p>
<p><b>Related Threats</b></p>	<p>Malicious actions, human errors, system failures</p>

**GP 29. Establish dedicated access control mechanisms for medical device facilities**

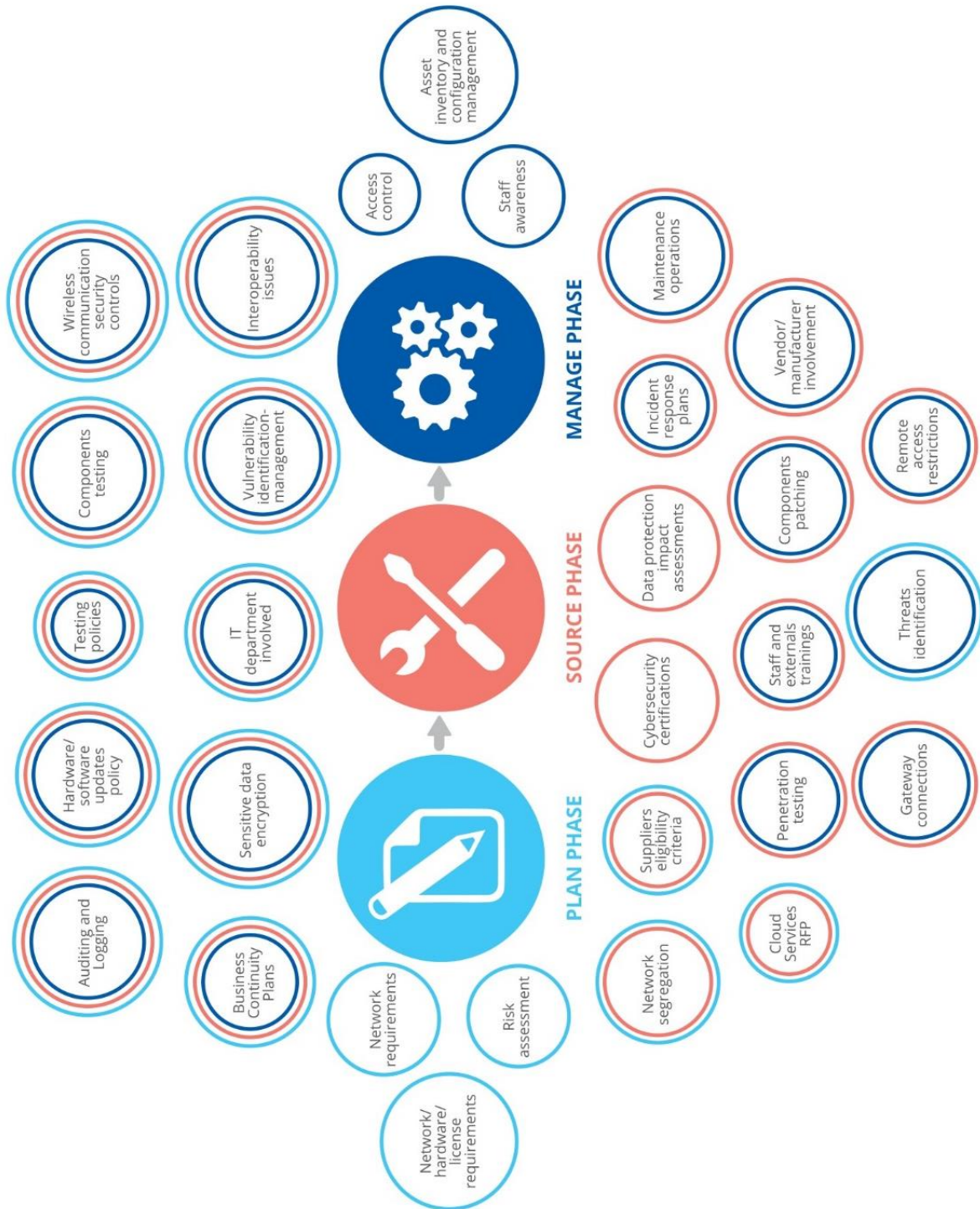
	<p>Medical devices such as PET/ CT scanners, surgical robots etc. should be also physically protected. Access should be allowed only for specialised personnel and each one should have a dedicated account. The IT department should monitor the access control policy of each device. When procuring devices these provisions should be taken into account by the supplier.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• Role based access control, dedicated accounts for the ones handling medical devices with strict controls (blocking access after 2 wrong entries, 2 factor authentication etc.)</li> <li>• Establish physical access control measures for medical device facilities (access using biometrics). Technical description should include this provision</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Medical devices, building management system, identification systems</p>
<p><b>Related Threats</b></p>	<p>Malicious actions, Human error</p>

**GP 30. Schedule penetration testing frequently or after a change in the architecture/ system**

	<p>The supplier recognizes the hospital's right to carry out necessary security checks (e.g. security audits, penetration tests) under its own authority and shall guarantee unrestricted access to the necessary documents to the institution or to the hospital's authorized representative. A specific clause should be included in the RfP.</p> <p>It is also important to note that a newly acquired or newly configured product must undergo a penetration test in its actual installed environment.</p>
<p><b>Examples/ Evidence</b></p>	<ul style="list-style-type: none"> <li>• It is important for products and systems to be tested once they have been installed and configured at their actual operating environment. Any issue remediate actions that will follow should take into consideration the specific operational parameters of this environment.</li> <li>• The supplier should (if required in the RfP) offer options for penetration testing by a third party. This should include both black and white box testing. The supplier should include the cost of these test in the offer</li> <li>• The hospital has the right to request the results of audits performed in the supplier's side. The supplier should inform in case of a test and enhance transparency</li> </ul>
<p><b>Related Procurement Types</b></p>	<p>Medical Devices, Clinical Information Systems, Networking Equipment, Remote Care System, Mobile Client Devices, Identification Systems, Industrial Control Systems, Cloud Services</p>
<p><b>Related Threats</b></p>	<p>Malicious Actions, Supply Chain Failure, System Failures</p>

# 5. OUTLOOK

Figure 5: Good practices for cybersecurity in procurement for Hospitals



# A ANNEX: INDUSTRY STANDARDS

**Table 4:** Standards related to the manufacturing of medical devices

Standard	Description
ISO 13485	<p>ISO 13485 defines the requirements that a quality management system must meet for the design and manufacture of medical devices.</p> <p>This regulation is based to some extent on ISO 9001. ISO 13485 requires only that the certified organization demonstrate the quality system is effectively implemented and maintained and is often seen as the first step in achieving compliance with European regulatory requirements.</p>
ISO 14971	<p>ISO 14971 establishes the standard recommended for medical device risk management to determine the safety of a medical device during the product life cycle. Such activity is required by higher level regulation (EU directives 93/42/EEC, 90/385/EEC and 98/79/EEC) and other quality management system standards such as ISO 13485.</p> <p>Technical report <b>ISO/TR 24971</b>, also from ISO, provides guidance on the application of this standard.</p>

**Table 5:** Standards related to the acquisition and management of health information systems

Standard	Description
ISO / IEC 20000	<p>The series ISO/IEC 20000 is the internationally recognized standard for Service Management in IT.</p> <p>ISO 20000 specifies requirements for "establishing, implementing, maintaining and continually improving a service management system [...] including planning, design, transition, delivery and improvement of services".</p>
ISO 27000	<p>ISO/IEC 27000-series provides best practice recommendations on information security management.</p>
ISO 27799	<p>ISO 27799 defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that International Standard.</p> <p>By implementing ISO 27799:2016, healthcare organizations will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information in their care.</p>
IEC 62304	<p>The international standard IEC 62304 is a standard which specifies life cycle requirements for the development of medical software and software within medical devices.</p> <p>It is harmonized by the European Union (EU) and the United States (US), and therefore can be used as a benchmark to comply with regulatory requirements from both these markets.</p> <p>Technical report <b>ISO/TR 24971</b>, also from ISO, provides guidance on the application of this standard.</p>
NIST-SP 800-66	<p><a href="#">Special Publication 800-66 Rev. 1</a>, it's a guide for implementing the Health Insurance Probability and Accountability Act (HIPAA) Security Rule, which discusses security considerations and resources that may provide value when implementing the requirements of the HIPAA Security Rule.</p>





<b>NIST CSF</b>	NIST CSF (NIST CyberSecurity Framework) provides a policy framework of computer security guidance for private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber-attacks.
<b>ISO 22857</b>	ISO 22857:2013 Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health data, provides guidance on data protection requirements to facilitate the transfer of personal health data across national or jurisdictional borders.  It is normative only in respect of international or trans-jurisdictional exchange of personal health data. However it can be informative with respect to the protection of health information within national/jurisdictional boundaries and provide assistance to national or jurisdictional bodies involved in the development and implementation of data protection principles.

**Table 6: Standards related to the communication between healthcare devices and the sharing of medical information**

Standard	Description
<b>ISO 80001</b>	ISO 80001 is the standard recommended for risk management in IT-networks incorporating medical devices.  It defines the functions, responsibilities and activities that are necessary for the IT-Network Risk Management to address safety, effectiveness and data and system security (the key properties).  This standard does not specify acceptable risk levels, however, risk management activities derive from the aforementioned standard, ISO 14971.
<b>ISO 15225:2016 (withdrawn)</b>	ISO 15225:2016 specified rules and guidelines for a medical device nomenclature data structure, in order to facilitate cooperation and exchange of data used by regulatory bodies on an international level between interested parties.  Included guidelines for a minimum data set and its structure. These guidelines are provided for system designers setting up databases that utilize the nomenclature system described herein.  The requirements contained in this International Standard were to be applicable to the development and maintenance of an international nomenclature for medical device identification.
<b>ISO 13972</b>	ISO 13972:2016 Health informatics — Detailed clinical models, characteristics and processes defines Detailed Clinical Models (DCMs) in terms of an underlying logical model.
<b>ETSI eHealth standards</b>	The European Telecommunications Standards Institute (ETSI) is an independent, not-for-profit, standardization organization in the telecommunications industry (equipment makers and network operators) in Europe, headquartered in France.  ETSI Project (EP) eHEALTH is “committed to the creation of a technical standards-based market for health. It will promote a climate of innovation, underpinned by technical standards to ensure interoperability, efficiency, security, privacy and safety in the provision of health services worldwide”.
<b>HL7</b>	Health Level Seven or HL7 refers to a set of international standards developed by HL7international that is becoming increasingly popular. HL7 provides a comprehensive framework and related standards for transfer of clinical and administrative data in a uniform and consistent manner between software applications of health organizations.  <b>HL7 is the standard ISO/HL7 27931:2009 [HL7 RIM R1 - 2003] Data Exchange Standards — Health Level Seven Version 2.5 — An application protocol for electronic data exchange in healthcare environments.</b>
<b>DICOM</b>	Digital Imaging and Communications in Medicine (DICOM) is the most widely used standard for the communication and management of medical imaging information and related data. DICOM is most commonly used for storing and transmitting medical images to Picture Archiving and Communication Systems (PACS) from multiple manufacturers. DICOM defines the formats for medical images that can be exchanged with the data and quality necessary for clinical use.

	<p>Its derived ISO standard, <b>ISO 12052:2017</b>, within the field of health informatics, addresses the exchange of digital images and information related to the production and management of those images, between both medical imaging equipment and systems concerned with the management and communication of that information.</p>
<p><b>NIST NISTIR 7497.</b></p>	<p>NIST NISTIR 7497: also known as <a href="#">The Health Information Exchange (HIE) Security Architecture</a> defines guidelines to provide a systematic approach to designing a technical security architecture for the exchange of health information.</p>

**Table 7: Standards related to the provisioning of Industrial Control Systems**

Standard	Description
<p><b>ISO 27019</b></p>	<p>ISO/IEC TR 27019:2013 provides guiding principles based on ISO/IEC 27002 for information security management applied to process control systems as used in the energy utility industry.</p>
<p><b>IEC 60364-7-710</b></p>	<p>IEC 60364-7-710 applies to electrical installations in medical locations, to ensure the safety of patients and medical staff. Its requirements mainly cover hospitals, private clinics, medical and dental practices, health care centres and dedicated medical rooms in the workplace.</p>
<p><b>UK Health Technical Memoranda (HTMs)</b></p>	<p><a href="#">Health Technical Memoranda</a> (HTMs) give comprehensive advice and guidance on the design, installation and operation of specialised building and engineering technology used in the delivery of healthcare.</p> <p>The series contains a suite of nine core subjects:</p> <ul style="list-style-type: none"> <li>00: Policies and principles (applicable to all Memoranda)</li> <li>01 Decontamination</li> <li>02 Medical gases</li> <li>03 Heating and ventilation systems</li> <li>04 Water systems</li> <li>05 Fire safety</li> <li>06 Electrical services</li> <li>07 Environment and sustainability</li> <li>08 Specialist services</li> </ul>
<p><b>ISA/IEC 62443</b></p>	<p>Developed by the ISA99 committee, ISA-62443-4-2, Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components, provides the cybersecurity technical requirements for components that make up an IACS, specifically the embedded devices, network components, host components, and software applications.</p> <p>The standard, which is based on the IACS system security requirements of ISA/IEC 62443-3-3, System Security Requirements and Security Levels, specifies security capabilities that enable a component to mitigate threats for a given security level without the assistance of compensating countermeasures.</p>



## ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at [www.enisa.europa.eu](http://www.enisa.europa.eu)

### ENISA

European Union Agency for Cybersecurity

#### Athens Office

1 Vasilissis Sofias Str  
151 24 Marousi, Attiki, Greece

#### Heraklion office

95 Nikolaou Plastira  
700 13 Vassilika Vouton, Heraklion, Greece

[enisa.europa.eu](http://enisa.europa.eu)



ISBN 978-92-9204-312-4  
DOI: 10.2824/943961