EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CLOUD SECURITY FOR HEALTHCARE SERVICES

JANUARY 2021

ABOUT ENISA

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

CONTACT

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

AUTHORS

Dimitra Liveri, Dr. Athanasios Drougkas, Antigone Zisi, EU Agency for Cybersecurity

ACKNOWLEDGEMENTS

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

Belani Hrvoje, Croatia Ministry of Health, Croatia

Bezouška Tomáš, Ministry of Health of the Czech Republic, Czech Republic

Calcavecchia Franck, Hôpitaux Universitaires Genève, Switzerland

Callewaert Frank, Microsoft, Belgium

Carbonell Marta, Hospital Universitary Vall d'Hebron, Spain

Chondropoulos Konstantinos, General Hospital of Thessaloniki "George Papanikolaou", Greece

Drost René, NAMCO, Netherlands

Gioulekas Fotios, University Hospital of Larissa & 5th Regional Health Authority of Thessaly and Sterea, Greece

Greenfield Søren Bank, Danish Health Data Authority, Denmark

Haro Albert, Cybersecurity Agency of Catalonia, Spain

Ikäheimonen Merja, Essote ky, Finland

Kirkmann Perit, Information System Authority, Estonia

Kokx Ben, Philips, Netherlands

Liebscher Thomas, Philips, Netherlands

Marek Dominik, Vysočina Region Regional Authority, Czech Republic

Meany Ben, Microsoft, Belgium

Pennings Florian, Microsoft, Belgium

Rad Abtin, TUEV SUED Product Service GmbH, Germany

Smethurst Chelsea, Microsoft, Belgium

Starolis Saulius, National Health Insurance Fund under the Ministry of Health, Lithuania

Tzikas Athanasios, University Hospital of Larissa, Greece

Žukovskis Raivis, The National Health Service of the Republic of Latvia, Latvia

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), 2021
Reproduction is authorised provided the source is acknowledged.

Copyright for the image on the cover: © Shutterstock
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 978-92-9204-405-3, DOI 10.2824/454966

LIST OF ABBREVIATIONS

Abbreviations	Definitions
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface
AWS	Amazon Web Services
BSI	British Standards Institution
CCN	Centro Criptológico Nacional
CDS	Clinical Decision Support
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMMC	Cybersecurity Maturity Model Certification
COVID	Corona Virus Disease
CSA	Cloud Security Alliance
CSP	Cloud Security Provider
DP	Data Protection
DSI	Digital Service Infrastructure
EC	European Commission
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EFTA	European Free Trade Association
EHR	Electronic Health Record
ERP	Enterprise Resource Planning systems
EU	European Union
GDPR	General Data Protection Regulation
GP	Good Practice
HCO	Health Care Organisation
HDS	Hébergeurs de Données de Santé
HDSI	Health Digital Service Infrastructure
HIPPA	Health Insurance Portability and Accountability Act
HIS	Health Information Systems

HITRUST	Health Information Trust Alliance
IACS	Industrial Automation and Control Systems
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IMDRF	International Medical Device Forum
JASEHN	Joint Action to Support the eHealth Network
LIS	Laboratory Information System
MS	Member States
NISD	Network and Information Security Directive
NIST	National Institute of Standards and Technology
OS	Operating System
OWASP	Open Web Application Security Project
PACS	Picture Archiving and Communication System
PHP	Hypertext Pre-processor (scripting language)
RIS	Radiology Information System
RPM	Remote Patient Monitoring
SLA	Service-Level Agreement
SM	Security Measure

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The healthcare sector is going through the digitalisation process and continuously adopting new technology to improve patient care, offer new services focusing on patient-at-home care, and reach operational excellence. The integration of new technology in an already complex IT infrastructure opens up new challenges regarding data protection and cybersecurity. Moreover, the ongoing COVID-19 pandemic has been a further catalyst for cyberattacks on healthcare organisations[1,2,3]. Typical examples are phishing attacks that aim to collect user credentials of healthcare professionals and ransomware[4] against hospitals and other Healthcare Organisations (HCO).

At the same time this pandemic stresses the need for remote healthcare services, since the system was overwhelmed in some countries and physical presence was a risk for the spread of the pandemic. In this context, Cloud solutions have provided elasticity and fast access for the deployment of new services including «virtual» health and telemedicine.

This study aims to provide Cloud security practices for the healthcare sector and identify security aspects, including relevant data protection aspects, to be taken into account when procuring Cloud services for the healthcare industry.

The set of general practices aims to help IT professionals in the healthcare security contexts to establish and maintain Cloud security while selecting and deploying appropriate technical and organisational measures. The identification of relevant threats and risks to Cloud services in the healthcare industry and security and data protection requirements are also covered by the scope of this report. Further objectives include the presentation of informative and practice-oriented use cases and their analysis of relevant threats and Cloud security measures.

The overall conclusion derived from the study, is that Cloud integration in the healthcare sector in the EU is still in its infancy. Some healthcare organisations hesitate to adopt Cloud services, because they are challenged by a dense and complex legal basis, and new technologies. Furthermore, the loss of data governance and processing of personal data in the Cloud makes healthcare organisations hesitant to adopt Cloud services. Other healthcare organisations use PaaS for connecting medical devices with a web-application for remote monitoring of patients or SaaS for documentation and scheduling doctor-patient consultations. Some countries are in the beginning of forming a Government Cloud (G-Cloud) to satisfy such needs. There are also various government managed services such as electronic prescription and electronic health records, which run on government-owned resources, such as private Clouds and state owned datacentres and Clouds.

The study is structured around three use cases, which are the most prominent in using Cloud or to be using in the future, namely Electronic Health Record, Remote Care and Medical Devices. A set of 17 security and data protection measures has been identified to be relevant for ensuring Cloud security and have been assessed based on the use case.

[1] https://www.verdict.co.uk/healthcare/
[2] https://healthitsecurity.com/news/covid-19-impact-on-ransomware-threats-healthcare-cybersecurity
[3] https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far
[4] https://us-cert.cisa.gov/ncas/alerts/aa20-302a

1. INTRODUCTION

1.1 CONTEXT OF THE REPORT

The healthcare sector is one of the sectors most vulnerable to cyber attacks[5]. Simultaneously, the digitalisation of the healthcare sector is moving forward, and digital solutions or electronic records continuously replace paper-based processes. The transformation affects services along the complete healthcare delivery chain, i.e. medication, appointment scheduling, patient records, inpatient and outpatient care as well as inpatient and remote monitoring or self-management.

COVID-19 pandemic indicated how vulnerable the healthcare sector is to cyberattacks and the need for "tele" medicine also as a more secure solution.

Digitalisation offers new solutions to improve patient care and gain operational excellence in healthcare organisations. Cloud solutions for healthcare services offer an excellent opportunity to increase operational efficiency, cut costs on IT expenditure and improve cybersecurity and data protection. This is since Cloud service providers have resources such as personnel, knowledge of technology, and the financial means to improve cybersecurity and data protection continuously. These are the same factors that sometimes have proven to hinder advances in the maturity of data protection and cybersecurity at healthcare organisations.

The COVID-19 pandemic has pushed Cloud-based technology usage in the healthcare sector, especially in telemedicine, for patient-doctor consultations and artificial intelligence for triaging purposes. The further integration of Cloud computing services in the healthcare sector also raises security and data protection concerns. This report therefore aims to help ensure Cloud security for healthcare.

1.2 OBJECTIVE

This report's overall objective is to provide the target audience with a set of guidelines to ensure cybersecurity and security of personal data processing when procuring Cloud services for providing healthcare services and a clear understanding of the corresponding responsibilities. The goals are to provide an overview of the landscape of the applicable EU legislative instruments relevant to Cloud services in the healthcare sector and the main cybersecurity and data protection challenges, relevant to security of personal data processing, of Cloud customers from the healthcare sector.

1.3 SCOPE

The study's scope is Cloud services that support the broader eHealth ecosystem, such as healthcare services and facilities, medical devices and equipment, medical services, or managed care. It is not limited to a specific Cloud architecture, neither deployment nor service model. The study focuses on showing relevant threats, measures, and responsibility by analysing three representative use cases, electronic health record, remote care, and medical devices.

The set of guidelines for Cloud security of healthcare services (output) is primarily for Cloud customers, such as healthcare organisations or medical device manufacturers. The study, investigation, and the output are centred on the European Union and European Free Trade Association (EFTA) member states.

[5] IBM, X-Force Threat Intelligence Index, 2020, pp. 39., see also Moore, J., Which sectors are most vulnerable to cyber attacks, 2020. https://www.ifsecglobal.com/cyber-security/which-sectors-are-most-vulnerable-to-cyber attacks/

1.4 TARGET AUDIENCE

The target audience of the study's output acceptable practices for ensuring Cloud security for healthcare services is anyone interested in using Cloud technology in the healthcare sector. The main focus is on Cloud customers in healthcare, primarily:

- IT health professionals (CISO, CIO, IT procurement specialists, and IT-teams in charge of purchasing Cloud services)
- Healthcare professionals in managerial positions seeking advice on whether to procure Cloud services

The report may be useful to IT professionals from medical device manufacturers and possibly, policymakers and Cloud service providers.

1.5 METHODOLOGY

The applied methodology of this study comprises four steps.

- **Step 1 Desk Research:** Extensive desk research for gathering information identifying Cloud services supporting healthcare services, Cloud security threats, and security controls for providing Cloud security for healthcare in general and during the procuring process.
- **Step 2 Questionnaire and semi-structured interviews:** Experts and representatives from the healthcare and Cloud technology industry of ENISA's expert network have provided information on Cloud-based healthcare services, its associated risks and opportunities, Cloud security and cybersecurity requirements in general, and implemented or identified cybersecurity and data protection measures from their point of view. Interviews have been conducted to collect additional valuable input from the experts.
- **Step 3 Analysis**: The analysis of the results from step 1 and step 2 provides input for the report and its objectives. This step supports the identification of security challenges and the validation of the use cases. Based on the analysis results, the first draft of the report has been drafted.
- **Step 4 Review and validation:** The last step comprises the review and validation by ENISA's expert group. The final version of the report is drafted, taking into account the feedback from the experts.

1.6 STRUCTURE OF THE DOCUMENT

The report is structured as follows:

- **Section 1 – Introduction** provides introductory information on the report and describes the scope, objectives, target audience, and the applied methodology.
- **Section 2 – Cloud Services in Healthcare** outlines Cloud service terminology, characteristics, and responsibilities. It includes an overview of Cloud services in healthcare identified through desk research and interviews.
- **Section 3 – Cybersecurity considerations in Cloud for Healthcare** entails cybersecurity and data protection considerations for the use of Cloud for healthcare services. It also includes a threat taxonomy based on the ENISA procurement guide.
- **Section 4 – Use cases** shows a description of the possible use cases, the factors to be considered when conducting the respective risk analyses in terms of risk likelihood and impact, and appropriate security measures, relevant to personal data processing, for risk mitigation.
- **Section 5 – Cloud security measures in healthcare** lists and presents measures for ensuring Cloud security for healthcare services, including additional data protection considerations.

2. HEALTHCARE IN THE CLOUD

2.1 POLICY CONTEXT

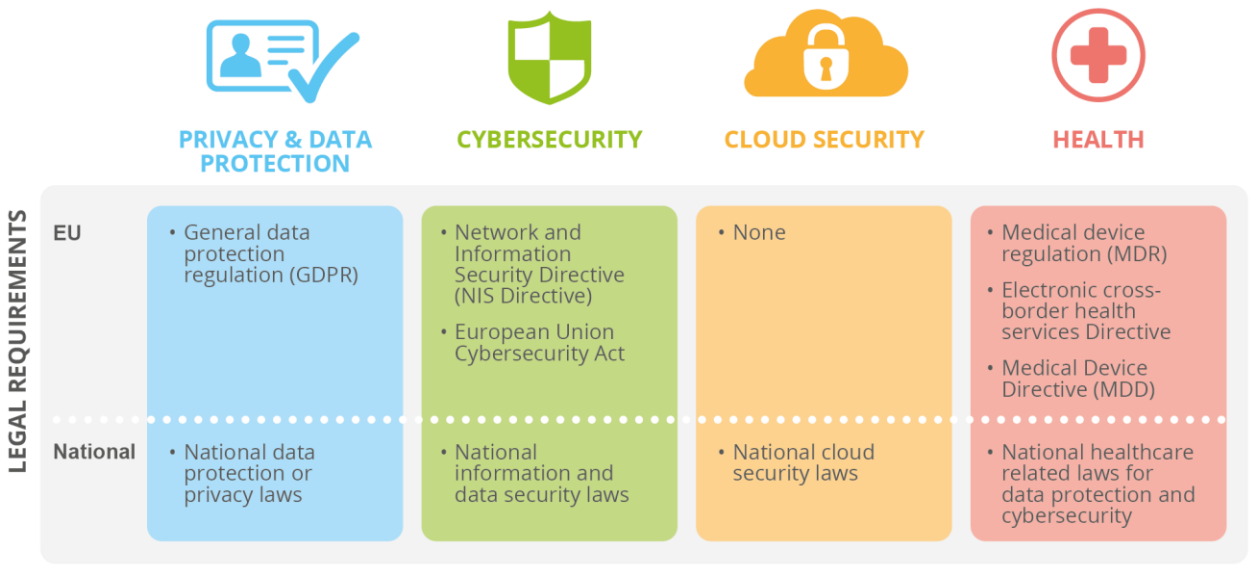
Legislation plays an important role in defining cybersecurity requirements and adopting cybersecurity and data protection related measures. In the case of healthcare and the Cloud, the policy landscape at national or European level is still at early stages of development. Very few MS have Cloud-related guidelines specifically for the healthcare sector, simply because if Cloud security guidance is in place, it applies to all critical sectors; all Member States consider healthcare a critical sector.

The general conclusion derived from the desk research and expert interviews shows that MS have a dedicated legislation for healthcare activities (not necessarily covering cybersecurity) and in several cases they adopt cybersecurity guidelines for Cloud computing; there is no case of healthcare and Cloud specific legislation. This corresponds to the assessment of the healthcare sector as critical, thus required to abide by overall cybersecurity legislations and guidelines.

At the same time, identification of requirements deriving from national or European legislation, proves crucial when procuring Cloud services. Some healthcare services, electronic health records for instance, have a separate law entailing security and data protection requirements. And eventually, to some extent the general practices overlap.

The illustration below depicts the legislative situation regarding Cloud security and healthcare. From a legal requirements perspective, we examined four topic-related dimensions: privacy, cybersecurity, Cloud security, and healthcare.

Figure 1: Legislations related to Cloud security and healthcare



The most relevant legal documents or guidelines at EU level are summarised below.

2.1.1 The Network and Information Security Directive (NISD)

The Network and Information Security Directive (NISD) 2016/1148/EU[6], 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. At the same time Cloud Service Providers are considered Digital Service Providers. Therefore, both these types of organisations will have to take the Directive and the relevant national law into account when contracting a Cloud 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 organisation is acceptable and as per the provisions of the Directive. At the same time, the Directive puts in scope specific services which span among the designated essential sectors. In the healthcare ecosystem, this can be translated as cybersecurity requirements for all products so it should be included as a provision in the procurement process.

For the Digital Service Providers, the decision on the details of cybersecurity measures resides with the MS, since the Directive leaves a certain level of flexibility. In the case of Cloud services offered to an operator of essential healthcare service, both parties need to agree on how the legal requirements will be met before reaching a contractual agreement.

2.1.2 General Data Protection Regulation

The General Data Protection Regulation (GDPR)[7] 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, aimed 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.

The GDPR considers 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 processing. Organisations (Data controllers) 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 them.

The GDPR expanded the scope of application of EU data protection law requirements to the data processors as well. This means that Cloud service providers, acting as data processors on behalf of the data controller, have obligations as data controllers but their obligations would not necessarily be the same.

2.1.3 Non regulatory guidelines

Prior to the adoption of GDPR, in 2012, the European Data Protection Supervisor (EDPS) had issued an opinion on the use of Cloud Computing and provided guidance indicating security measures for data protection but also sharing considerations in respect to responsibilities

[6] https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[7] https://eur-lex.europa.eu/eli/reg/2016/679/oj

between data processor and data controller. This can be used as a basis for Cloud security requirements solicitation from the healthcare sectors as well.

In 2015, the Joint Action to Support the eHealth Network (JASEHN) issued a report[8] on the use of Cloud computing in health focusing primarily on the secondary use of health data where amongst other explains the responsibility shift between the HCO and the CSP based on the service model (IaaS, PaaS, SaaS etc).

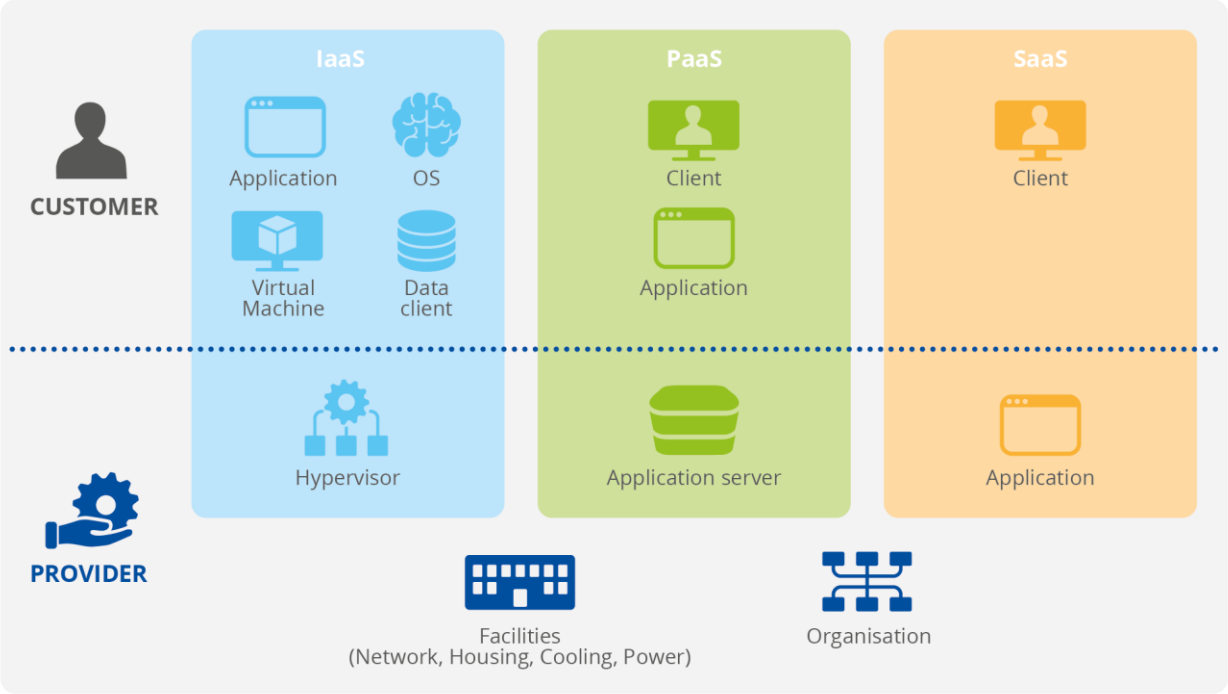
In 2018, the European Data Protection Board (EDPB) and the EDPS issued an opinion[9] specifically for healthcare namely on data protection for eHealth Digital Service Infrastructure compiled under the directive on patients' rights to cross-border healthcare. Amongst other things, the opinion includes requirements for more secure information exchange (i.e. encryption), secure data storage and that the EC, as data processor, has to clarify the governing rules of the processing.

2.2 CLOUD COMPUTING BASICS

2.2.1 Cloud Services

As per previous ENISA publications[10], the basic types of Cloud services can be explained in the following diagram:

Figure 2: Basic types of Cloud services



Interpreting the diagram from left to right:

- Infrastructure as a Service: In IaaS, the provider delivers computing resources (virtual hardware), accessible online. The software providing access to the resources is called the hypervisor. Generally speaking there are two types of resources: processing power

[8] https://webgate.ec.europa.eu/chafea_pdb/health/projects/677102/outputs
[9] https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-opinion-ehdsi_en
[10] https://www.enisa.europa.eu/topics/cloud-and-big-data

(including network resources), and (block) storage (memory resources). Examples include Amazon's Elastic Compute Cloud, Google's Compute Engine, Amazon Simple Storage Service, Dropbox, Rackspace, etc. Note that object storage services (e.g. Dropbox) are often considered SaaS.

- Platform as a Service: In PaaS, the provider delivers a platform, or more precisely, application servers, for customers to run applications on. PaaS providers sometimes provide a software development tool for the platform. Examples of applications running on these platforms are scripts (PHP, Python, e.g.) or byte code (Java servlets, C#). Examples include Google App engine, Microsoft Azure, Amazon Elastic Beanstalk, etc.

- Software as a Service: In SaaS, the provider delivers full-fledged software or applications, via the internet. Applications range from email servers, document editors, customer relationship management systems, and so on. SaaS services can often be accessed with a browser or a web services client. Note that it is not uncommon for SaaS providers to run their applications on an IaaS or PaaS from another provider. An example is the video streaming site Netflix (SaaS) which runs on Amazon AWS computing services (PaaS/IaaS).

- Facilities denote the physical structures and supplies such as networks, cooling, power, etc.

- Organisation denotes the human resources, the policies and procedures for maintaining the facilities and supporting the delivery of the services.

2.2.2 Cloud Deployment models

Private Cloud is a model in which one customer has exclusive access to the Cloud infrastructure and computational resources, that can be hosted by the customer itself or a provider, over a private network.

Public Cloud refers to a shared Cloud infrastructure and computational resources that are available and reachable over the public internet.

Hybrid Cloud is a model for a group of users that share the same Cloud infrastructure and the computational resource. The premises may be owned, managed, and operated by one or more of the organisations in the community, a third party, or both. It may exist on the community's location (on-site) or the third-party's location (off-site).

Governmental Cloud (g-Cloud) is a Cloud environment where the Cloud infrastructure is owned, governed and run by the government or a state-owned entity using own resources or a selected third-party provider. In addition, the governmental Cloud enables the public body to provide services to public sector stakeholders, to citizens and enterprises.

For the purpose of this report, the definition of governmental Cloud is presented based on ENISA's reports[11].

2.2.3 Division of responsibilities

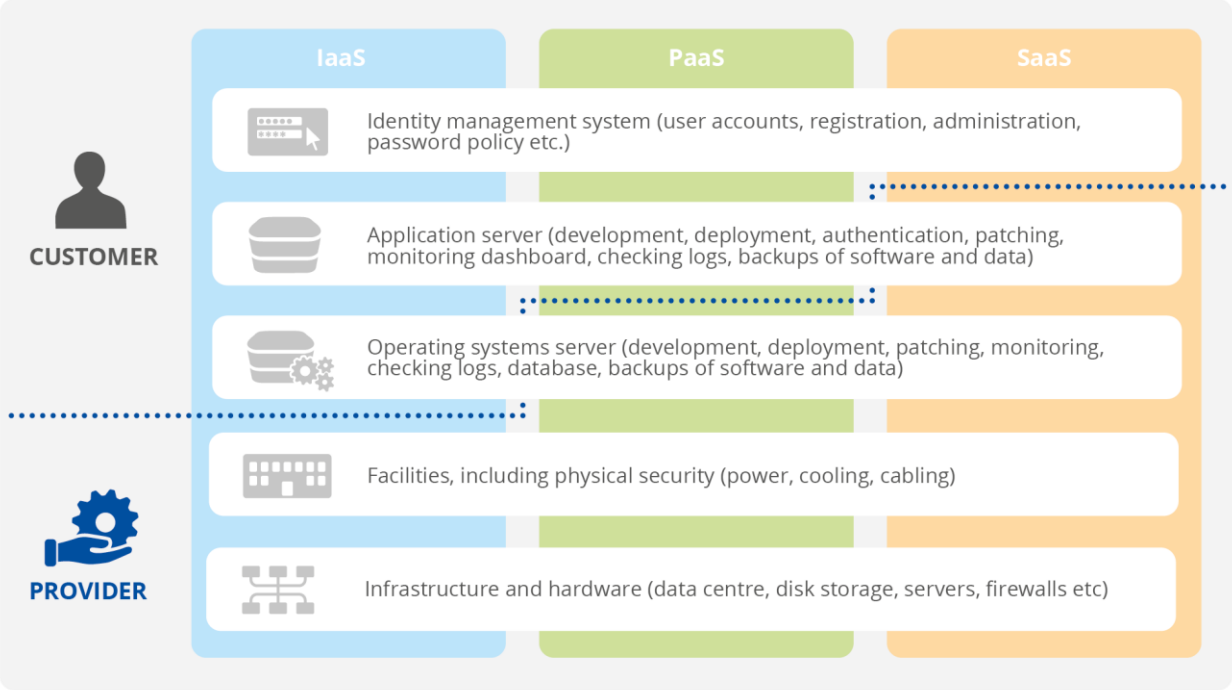
Similarly depending on the service model selected, the responsibilities might lie either on the side of the customer or of the provider; the higher you move in the service stack as a customer the fewer technical responsibilities one has to implement. Note that this diagram is for illustration only and does not provide an exhaustive list of security processes on the provider's or the customer's side. In specific settings there may be specific agreements about the

[11] https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

outsourcing of security tasks. An IaaS provider, for example, might have a service for patching the Operating System (OS) of customers. Sometimes such services are offered by a third-party (and this is also known as Security-As-A-Service or SECaaS).

At this point, it needs to be stressed that cybersecurity is always a shared responsibility- so regardless of the service model acquired, the customer always has a role in the cybersecurity or privacy requirements adoption.

Figure 3: Division of responsibilities of Cloud services



From the data protection perspective, the definitions and most likely assignment of roles are as follows:

- **Data controller**: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" GDPR Art. 4(7).

- **Data processor**: "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" GDPR Art. 4 (7). Depending on the service model (IaaS/PaaS/SaaS), the data processor might be the CSP or the customer. The higher a healthcare organisation moves up the Cloud services stack, the more processing power the Cloud provider has.

2.3 TYPES OF CLOUD SERVICES IN HEALTHCARE

In the healthcare sector, Cloud solutions exist for different healthcare services and their number is increasing. In this chapter, we provide a non-exhaustive overview of the currently identified Cloud solutions for healthcare systems. These solutions may come in different cloud service types (e.g. SaaS, PaaS etc.) or cloud deployment models. The following descriptions focus primarily on the types of functions and services supported by existing cloud services as opposed to the deployment models and relevant architectures.

Table 1: Non-exhaustive overview of the currently identified Cloud solutions for healthcare systems

Type of cloud services	Description
Enterprise resource planning systems (ERP systems)	Enterprise resources planning systems support the management of patients, appointments, medical staff's schedules and inventory. Dedicated parts of an ERP system could be available as Cloud-based solutions, for instance: • Patient management system • Health insurance management • Billing and human resource management • Other non-clinical data management
Health information systems (HIS)	Health information systems are used for managing healthcare data and entail demographic and medical patient data, which comprise records, images, or even videos. In the area of health information systems, the following types are available or used as a Cloud-based solution: • Electronic health record (EHR) • Picture archiving and communication system (PACS) • Electronic prescription information system • Radiology information system (RIS) • Laboratory information system (LIS) • Clinical decision support (CDS) • Remote patient monitoring (RPM)
Communication services	Middleware is a communication service to transfer data between systems or devices with a different physical location. For instance, in a Cloud-based solution for a remote monitoring solution, only the transfer from the device to the electronic health record is Cloud-based with the medical data being stored at a data storage facility in the healthcare organisation.
Office management	Healthcare organisations use Cloud-based file servers for document archiving or mail servers for internal and external communication.
Cloud-based network	Cloud-based networks enable healthcare organisations to share infrastructure on an as-needed basis; therefore, having more flexibility if more resources in particular situations are required.
Health data analytics	Health data analytics need a lot of computing power. Healthcare organisations outsource this task with Cloud technologies. Artificial intelligence[12], machine learning is used to support medical research, diagnosis (e.g. cancer[13] or cardiac pathology[14]), data analysis (e.g. glucose measurement), treatment recommendation, and patient engagement. The use of Cloud computing technology for this area is continuously evaluated.
Medical devices	Medical devices identify data that can be accessed through a mobile app or a web-based platform from different stakeholders. The healthcare services provided using Cloud-based medical devices are blood pressure measurement using electronic stethoscope[15], glucose measurement, and electrocardiogram. The goal is to enable patients to measure heart rates or insulin level at home while the data is directly available to healthcare professionals for treating or scheduling an appointment. Diagnostic cameras that support healthcare professionals during the diagnosis also belong to this category.
Telemedicine services	Telemedicine is a healthcare service provided using telecommunication technology. The areas of application comprise of teleconsultation and tele assistance using conference or video-conference tools.
Medication monitoring	Medication assistance[16] supports patients following their medication through real-time monitoring. It is a further remote healthcare technology application[17] together with telemedicine and medical devices.
Supply chain management	Supply Chain Management guarantees the timely availability of safe medical devices for use in the healthcare processes. This includes equipment, implants, disposables and medical software.

[12] Davenport and Kalakota, 2019
[13] Junaid Ahmad, Vinai, Bilal, 2015 and Sadhasivam, Balamurugan, and Pandi, 2018
[14] Agliari et al., 2020
[15] Leng et al. 2015
[16] Ventsislav and Rosen, 2016
[17] Cavoukian et al., 2010

3. CYBERSECURITY CONSIDERATIONS IN CLOUD FOR HEALTHCARE

3.1 CLOUD SECURITY CHALLENGES FOR HEALTHCARE

In this section, we present the main challenges regarding Cloud security, derived from the input of different experts collected through interviews. Even if the list is not exhaustive, the identified challenges comprise trends and obstacles regarding cybersecurity and data protection of the healthcare sector and the risks from Cloud-based healthcare services.

- **Lack of trust of Cloud solutions**: Overall, it has become evident that stakeholders in the healthcare sector (patients, physicians, medical staff, and healthcare organisation management) indicated a lack of trust of Cloud solutions. For example, patients' concern for their medical data being stored at the facilities Cloud service provider is often reduced due to the pre-existing relationship of trust between patient and doctor and due to the higher valuation of the patient's health over data protection and cybersecurity. In the case of medical staff, they tend to be less aware of cybersecurity and data protection. Therefore, it is a challenge to raise awareness for security-related topics and train in new authentication or identification technology. Also, human resources do not need to necessarily understand security and technologies- however they should be aware of the offerings of the Cloud providers in terms of that expertise. Without training and education, the occurrence of human errors and social engineering attacks is more likely.

- **Lack of security and technology expertise:** Moving the entire IT infrastructure or individual services from on site to the Cloud requires human resources that understand Cloud technologies and the associated security and data protection aspects. These knowledge requirements may not be covered by the same IT personnel responsible for the on-site infrastructure and eventually result in job termination. To migrate back from the Cloud to on-site infrastructure may be more challenging under such circumstances. Furthermore, the demand for Cloud security experts for the healthcare sector is higher than its supply, hindering Cloud computing advancement.

- **Cybersecurity investment is not a priority**: A lack of healthcare organisation management support or restricted public financing results in less financial support to further promote the digitalisation and to increase cybersecurity and data protection maturity in the healthcare sector.

- **Proving regulatory compliance of the CSP**: In several cases, Cloud customers have difficulty identifying which Cloud service provider is compliant with their set of legal requirements which sometimes limits their options for CSP collaboration. Assessment by the cloud customer of the Cloud provider's compliance is rarely possible or only with considerable financial resources. However, many CSPs provide this publicly via their compliance websites, and is often backed up from independent 3rd parties or even, sometimes, through government certification/assurance programs. In the other hand, regulatory requirements are so complex when it comes to healthcare-related data that CSPs do not even include these types of customers in their business model.

- **Integration of Cloud with legacy systems difficulties:** The integration of Cloud solutions with already existing healthcare organisation infrastructure or connecting several devices in-house and cross border, involves a great challenge and even results in refraining from using Cloud services. Moreover, in most cases, legacy systems are a part of health IT infrastructure. These systems are not supported by updates from their suppliers, which complicates integration and interoperability with new technology. Consequently, this makes these systems vulnerable to cybersecurity attacks. Hybrid deployment models allow a mix of health IT systems to partner with CSP services/solutions to deliver the most customizable needs to health care organisations. At the same time, the cost of deploying extra security features or integrating security elements with the on premise security perimeter is very high.

3.2 DATA PROTECTION CHALLENGES IN THE CLOUD

Similarly, in this section we present the main data protection-related challenges as derived from interviews with experts focusing mostly on the technical requirements for Cloud services in healthcare:

- **Privacy by design techniques**: The healthcare provider needs to understand whether the Cloud provider has followed a privacy-by-design approach (both policies and measures) when developing and deploying the service. The GDPR introduces a legal requirement on privacy by design and by default for both data controllers and data processors. Some of the techniques mentioned are minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing and enabling the controller to create and improve security features. Such approaches and strategies can be achieved through the use of particular technologies and policies, such as authentication, attribute-based credentials, secure private communications, anonymity and pseudonymity, statistical disclosure control, privacy preserving computations, and others[18].

- **Data management**: Healthcare organisations as authorised parties (after receiving consent) collect, structure and manage patient data. In some cases the information is automatically transferred to the Cloud (i.e. from a medical device) or it is input by a delegated party (i.e. medical practitioner). Depending on the type of service in the Cloud, the input information might be created by a different actor making accuracy of information a great issue. Controls for ensuring data accuracy should be in place, even if performed by third parties. Organisations need to establish their own data governance model/frameworks for understanding what kind of data is the most sensitive and then applying the required level of controls. Another issue to consider is interoperability, specifically for healthcare. This is a sector where Cloud computing brings many benefits due to its flexible range of services.

- **Data deletion**: It is extremely important to be able to erase data after retention time has expired, but also upon data subject's request without undue delay. The data subjects can substantiate their requests with one of the grounds foreseen in GDPR, such as when the data is no longer necessary for the initial purpose or when the data subject withdraws consent. Cloud providers have partially addressed the issue of identifying storage areas of chunks of information (data tagging). However, effective deletion of data is still a technical challenge.

- **Data portability**: This challenge goes hand in hand with vendor lock-in, the most common risk regarding Cloud Computing. Data portability refers to the transfer of one's

[18] https://www.enisa.europa.eu/publications/big-data-protection

data from one provider to another without loss upon their request. For healthcare certain standards are in place (like HL7) to ensure interoperability and thus portability.

- **Encryption**: One of the most important and at the same time difficult measures to implement is encryption. It is important to ensure secrecy and integrity but it has to be applied in all the different channels of data transfer and storage. Encryption measures need to be implemented at both client and server level but also in the channel that connects them. Responsibility then resides in both the Cloud customer and the Cloud provider and has huge implications from a technical and legal perspective. At the same time, few CSPs share the encryption keys with their customer leaving full control to the provider.

3.3 CYBERSECURITY THREATS

Following the threat taxonomy of ENISA's procurement guide[19] (ENISA, 2020), this section shows how the specific cybersecurity in healthcare can have implications for Cloud services.

Table 2: Cybersecurity Threats in healthcare and implications for Cloud services

High-level threat	Threat	Description
Natural phenomena	Fire, floods or earthquakes	Natural forces affect the Cloud infrastructure and eventually could result in a destruction of relevant systems, network components, or devices. Although the threat probability is low, the impact might be huge.
Supply chain failure	Cloud service provider failure	The Cloud services' availability is highly dependent on the Cloud service provider. Bankruptcy of the Cloud service provider, for instance, may threaten the continuous availability of the Cloud service, which may cause operational outages of healthcare organisations due to service failure. In the case of the Cloud provider's failure, a lack of data export and portability may result in loss of data. For all supply chain threats, redundancy and resiliency are critical topics the healthcare organisations should consider and inquire about.
Supply chain failure	Network provider failure	Network connection is crucial to access Cloud services. A network failure may impact Cloud-based healthcare service provision and affect the collaboration between different internal and external partners.
Supply chain failure	Power supply failure	Power supply can affect the Cloud service's availability, which may be critical when a pacemaker's data cannot be observed.
Human errors	Lack of tracing back functionality	Logs of activities in the Cloud service enable accountability, serve as evidence in the event of security incidents, and are used to investigate the causes of security incidents. The Cloud customer needs to ensure that logging is enabled based on risk. It also provides transparency for patients in the case of electronic health records.
Human errors	Unauthorised data access (information leakage)	Cloud users may gain unauthorised access to data due to insufficient access management or lack of awareness, which causes unintentional data disclosure. For example, a Cloud-based electronic health record has more users than a telemedicine solution.
Human errors	Non-compliance	Nowadays, the bring-your-own-device policy is widely applied in the healthcare sector, which causes variation in endpoint security. Measures to secure endpoints need to be adopted, and impacts on compliance, especially for accessing electronic health records, should be analysed.

[19] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

High-level threat	Threat	Description
Human errors	Unintentional change of data	Entering incorrect data into a healthcare system can result in loss of integrity and data disclosure to unauthorised users, such as uploading medical documents to the wrong electronic health record.
Human errors	Errors by Cloud service administrators/support staff	If data is not appropriately deleted from a Cloud storage or the backup media, the data may be accessed later by another Cloud customer of the same Cloud provider, and eventually result in a data breach. Configuration errors by Cloud service support staff may also leave vulnerabilities unpatched and leave entry points open for malicious attackers.
Malicious action	Malware injection attacks (i.e. virus, ransomware, worms)	Cloud environments are susceptible to malware injection attacks, which are a subcategory of web-based attacks. Attackers exploit vulnerabilities of a web application and embed malicious code into the normal action course. All Cloud service models are equally vulnerable to this kind of malicious action. Once the malicious code is executed, the attacker may eavesdrop, manipulate or steal data and instigate further attacks.
Malicious action	Hijacking	Hijacking infrastructure of the Cloud service provider to mine cryptocurrency (crypto-jacking) or a medical device (med-jacking) affects the patient's safety or the performance of the Cloud service healthcare provision. Hyper-jacking refers to hijacking the hypervisor using a virtual machine-based rootkit. Successful compromise of the hypervisor grants access to the entire machine and allows the compromise of the virtual machine.
Malicious action	Social Engineering attacks i.e. Phishing	Social engineering attacks to steal user credentials for SaaS solutions through phishing, spam, or spear-phishing emails are always targeted at the weakest link in the security chain, the human. On the whole, the healthcare sector is commonly known as less IT savvy and this raises the exposure to cyberattacks. Strong authentication provided by the Cloud service provider helps to prevent these kinds of attacks. Successful attacks could result in data breaches, data leakage, or data theft.
Malicious action	Account hijacking[20]	Account hijacking results from a malicious attacker gaining access to privileged accounts or sensitive accounts, such as Cloud service accounts or subscriptions. This threat can result in severe disruption of Cloud services and the provision of healthcare services.
Malicious action	Insecure interfaces and application programming interfaces	A Cloud computing environment provides user interfaces and APIs to interconnect devices and interact with the Cloud service. These interfaces offer an entry point for malicious attackers if they are poorly designed and lack security measures such as encryption and access control. Broken or hacked API's may result in data breaches.
Malicious action	Insider threat	Insiders can be current or former employees of healthcare organisations, contractors, or other trusted partners, who gain access from the inside of an organisation. These parties have had authorized access and may negatively affect the Cloud service and ultimately result in a data breach.
Malicious action	Isolation failure (Multi-tenancy)	In shared environments, errors or attacks may provide one tenant with access to another tenant's resources or data. A malicious attacker may gain access to one specific Cloud customer's resources or data or even all Cloud customers resulting in data breaches.

[20] Cloud Security Alliance, 2020

High-level threat	Threat	Description
Malicious action	Abuse of Cloud computational resources	Common examples of Cloud computing resource misuse are launching denial of service attacks, mining cryptocurrency, starting to propagate phishing or spam emails, and hosting malicious content in the Cloud environment. The abuse may affect Cloud services' availability or performance harming a patient's health.
Malicious action	Denial of service	Denial of service attacks against the Cloud service overload its resources due to a flood of requests originating from many sources and cause its unavailability and inability to process requests.
Malicious action	Intercepting data in transit (Man-in-the middle attack)	In a Cloud architecture model, data is transferred from the Cloud customer to the Cloud service provider. During transition, it may be intercepted and eventually result in a data breach.
Malicious action	Mobile application attacks[21]	Vulnerability in mobile apps running in the Cloud may also leave entry points open to be exploited by malicious attackers and result in data disclosure to unauthorised persons or even data loss.
System Failure	Network-related technical failures or attacks	Technical failures of network-related components influence the availability of Cloud service. Examples include the loss of Internet connectivity due to failures at the Cloud customer's or service provider's site, a temporary reduction of network bandwidth at the Cloud customer's internet service provider, which affects the data transfer from and to the Cloud service provider, and disruptions in the global Internet routing infrastructure capping the connection between the Cloud customer and Cloud service provider.
System Failure	Insufficient maintenance and maintenance procedures	Insufficient patch or life cycle management may occur at the Cloud customer's and the Cloud provider's sites. Failing to maintain the Cloud infrastructure and leaving software unpatched may result in disturbances or even failure of the Cloud service. Eventually, the patient's health may be affected due to unavailable medical records.
System Failure	Software failure	Due to errors, software failure can affect the Cloud services or medical device data availability and eventually endanger patient safety.
System Failure	Hardware failure	Failure of IT hardware at the Cloud service provider's or customer's site, limiting the Cloud service's availability, may severely impact patients' health in emergency cases. A medical device failure affects real-time data availability in the Cloud service possibly harming the patient's health.
System Failure	Deployment/ configuration Error	Technical failure related to system misconfiguration or interoperability issues in deployment. A cloud migration is a data centre migration, and it brings along all of the complexities that traditionally go along with one.

[21] OWASP, 2016

4. USE CASES

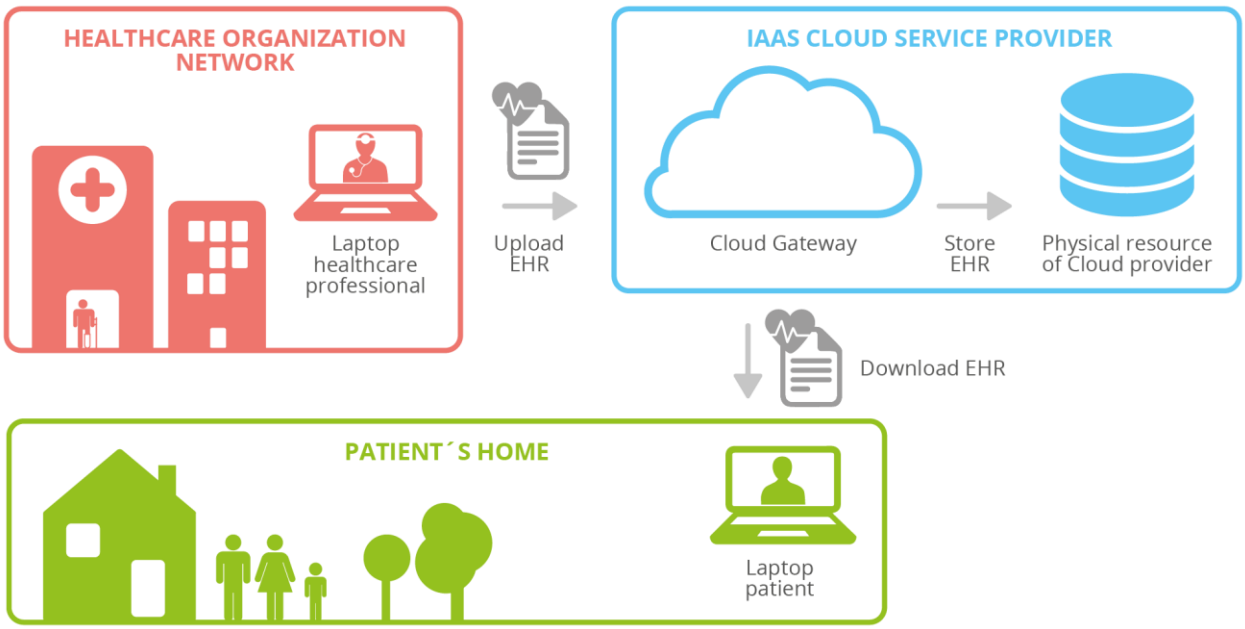
In this section, three use cases of Cloud services for healthcare are shown, including a reference Cloud architecture, factors to be considered during risk assessment, and risk mitigation measures.

4.1 USE CASE 1 - ELECTRONIC HEALTH RECORD

An electronic health record (EHR) provides services to a wide range of potential users: patients, doctors, nurses, public health officials, and more. These systems collect, store, manage and transmit sensitive health data such as patients' contact details, social insurance numbers, medical examinations' results, pathologies, allergies, diagnosis, and treatment plan. Healthcare professionals are provided with an overview of the history and the status of the patients' health and can access it if needed from pre-defined terminals within the healthcare provider's premises. After each examination or consultation, patient records are updated with the latest data by the treating doctor or nurse either by scanning paper-based documents or manually diagnosing and treatment plans.

Paper-based documents containing patient data are increasingly replaced with EHR in many countries, allowing health information to be shared in an easy-to-use and standardised way between different stakeholders such as healthcare professionals and patients. Solutions in this area often involve the use of Cloud computing resources or partially Cloud-based components. Patients can access and manage their EHR through a patient portal, which is usually integrated into Cloud solutions[22].

Figure 1: Cloud Architecture Model - Electronic Health Record (EHR)



[22] This is an exemplar case as not every EHR deployment uses governmental Clouds provided by the respective ministry. It is very common to see regional EHR deployments operated on public or private Clouds by public or private EHR providers. An EHR is typically sourced as SaaS and not at IaaS level but for the sake of completeness in this report, the specific service model is selected for the EHR.

OVERVIEW

Service Model	IaaS	**Deployment model**	Governmental Cloud
Healthcare organisation network		The healthcare organisation network is the Cloud customer of the governmental IaaS Cloud service provider. It is the body responsible for developing, maintaining, and deploying the application for sharing electronic patient records. Healthcare organisations upload the patient EHRs either through the web application or through an API, connecting their clinical information system with the corresponding national data centre in the Cloud. EHRs are stored at the national datacentre. Patients access their health records through the web application.	
Cloud service provider		The ministry of health, a government institution, provides the physical infrastructure for storing the EHRs. That includes, amongst others, the maintenance of the network infrastructure and the underlying operating systems.	

DEFINITION OF PROCESSING OPERATION AND ITS CONTEXT

Personal data processed	Contact information (patient's last and first name, address, telephone number, email address), contact information of relatives for emergency cases, social insurance number, medical appointments, medical examination results, pathologies, allergies, diagnosis and treatment plans (medical information), administrative and financial information (invoices, hospitalisation papers, etc.).
Processing Purpose	Provision of healthcare services (diagnosis, treatment, hospitalisation), treatment planning and billing
Data Subject	Patients, relatives, doctors, nurses
Recipients of the Data	Doctors and nurses, administration and accounting department, public health system, patients
Data Processor	IaaS Cloud service provider

ASSESSING CYBERSECURITY RISK IMPACT

When conducting a risk assessment for similar use cases, healthcare organisations should take into account the possible impact of a cybersecurity incident on confidentiality (e.g. data breach leading to exposed patient data), integrity (e.g. alteration of important patient data) or availability (e.g. timely access to patient data during emergency treatment). This would allow the healthcare organisation to assign an appropriate quantitative or qualitative value to the risk impact depending on the specific risk assessment methodology used. A brief description of factors to be considered for risk impact assessment is listed below:

Factor	Description
Confidentiality	Within the scope of the specific processing operation, the impact from loss of confidentiality is considerable given the nature of sensitive information included in the EHR. Data subjects could be expected to encounter significant adverse effects from unauthorised disclosure of their health data.
Integrity	The impact in case of loss of integrity should be considered particularly if the EHR includes important patient data that may be used to influence medical decisions. Data subjects may encounter significant or even irreversible consequences from unauthorised alteration of health data (signals and statistics), which could even make it difficult for them to receive appropriate treatment.
Availability	Depending on the nature of data included in the EHR and the context of their use, loss of availability may also be of significant impact. Inability to access the patient's EHR may hinder timely and accurate treatment of the data subjects, even putting their lives at risk.

ASSESSING RISK LIKELIHOOD

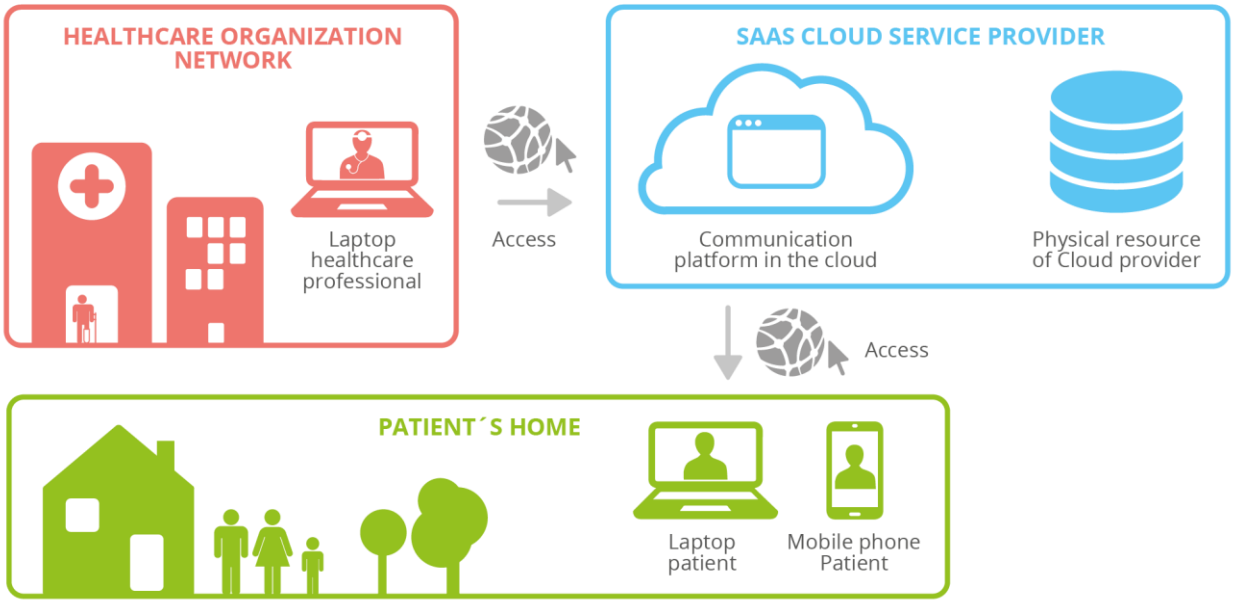
The table below describes how the main Cloud security threats may be relevant for the reference Cloud architecture and the specific use case. Healthcare organisations should use the information below when assessing the likelihood of a cybersecurity risk. It should however be noted that the descriptions below only refer to the described use case and additional factors related to the operational context of the healthcare organisation should be considered before determining the risk likelihood.

Threat	Description
Natural phenomena	Typically, in such use cases the servers are located in data centres enforcing a suitable level of physical security requirements, which tends to reduce the respective risk likelihood. Such data centres usually obtain certificates that show that they are protected against fire, water, or earthquakes and the existence of such certificates should be factored in the risk likelihood assessment.
Supply chain failure	As the infrastructure is outsourced to Cloud providers the likelihood of this risk tends to be reduced. The failure of power supply or other Cloud service disruptions is less likely because the providers are specialised in maintaining their services. However, even big Cloud platforms are not entirely immune to outages of their Cloud infrastructure.
Human error	An undefined number of employees may be performing personal data processing, and there is no clear policy regarding granular access to health records. This should be considered as a factor that increases risk likelihood. Human actors' common mistakes in this use case are the usage of default or weak passwords, lack of access control to sensitive data, non-compliance with security policies, or the possibility of human error. However, the obligations of all parties involved in the process should be clearly defined, and awareness-raising seminars should be organised periodically.
Malicious actions	Many parties such as healthcare organisations, patients, and public health officials are strongly interconnected in this Cloud system, which is difficult to isolate from malicious actors completely. Malicious attackers may also be internal actors who might have direct or indirect access to the Cloud services. Potential attacks in this area might involve social engineering (e.g., phishing), theft, espionage, malware (e.g., ransomware), or denial of service attacks. A database containing electronic health records of almost every citizen in a specific country stored centrally may be an attractive target for malicious attackers. On the other hand, Cloud service providers can bundle the knowledge of internal and external security experts, which allows them to enforce security measures more efficiently than proprietary data centres. These factors and especially the operational context of the healthcare organisation and the Cloud service provider should be assessed when determining the risk likelihood.
System failures	Software might have errors that cause the service to fail and become unavailable. The EHR is a very central solution to share patient information and is even legally regulated and requires security certification in most countries, reducing the occurrence probability. The government infrastructure typically also supports relevant governmental services that require a stable availability of the services. It can therefore be assumed, that the probability of system failures, especially hardware is usually relatively low. However, statistics on system failures or SLAs from the Cloud service provider can provide a more accurate source of data to feed into the risk assessment study.

4.2 USE CASE 2 – REMOTE CARE

Remote care (as part of Telemedicine) supports remote patient-doctor consultation and has been increasingly used in recent times due to the pandemic and its circumstances. During COVID-19, remote care/consultation has been a safe way to provide expert care and advice lowering infection risk. In some countries, remote care is an established approach to overcome centralised healthcare infrastructure and large distances. In this use case, we consider a service provider that offers a video call platform for communication between health professionals and its patients, individually or in group sessions. The service also offers recording, analysis, and transcription of the calls to assist the health professionals with medical evaluations, diagnosis, and documentation.

Figure 2: Cloud Architecture Model – Remote Care



OVERVIEW

Service Model	SaaS	**Deployment model**	Public Cloud
Healthcare organisation	The healthcare organisation uses a telemedicine (including audio and video) application for its doctor-patient consultation. The communication service is offered as a web and mobile application. The healthcare professionals connect over the internet using a client to access the Cloud service. Patients connect over the internet using either their computer or mobile phone.		
Cloud service provider	The Cloud service provider is a communication technology company offering a SaaS communication service. Its responsibility includes application development, maintenance, and providing the underlying infrastructure.		

DEFINITION OF PROCESSING OPERATION AND ITS CONTEXT

Personal data processed	Contact Information (last and first name, nickname), video recordings, transcriptions of recordings
Processing Purpose	Provision of healthcare services (patient-doctor consultation)
Data Subject	Patients/Medical professionals
Recipients of the Data	Medical professionals
Data Processor	SaaS Cloud service provider

ASSESSING CYBERSECURITY RISK IMPACT

When conducting a risk assessment for similar use cases, healthcare organisations should take into account the possible impact of a cybersecurity incident on confidentiality (e.g. data breach leading to exposed patient data), integrity (e.g. alteration of important patient data) or availability (e.g. timely access to patient data). This would allow the healthcare organisation to assign an appropriate quantitative or qualitative value to the risk impact depending on the specific risk assessment methodology used.
A brief description of factors to be considered for risk impact assessment is listed below:

Factor	Description
Confidentiality	Within the scope of the specific processing operation, the impact from loss of confidentiality can be considerable as the primary focus of such use cases involves the direct exchange of patient data. Data subjects may therefore encounter significant adverse effects from unauthorised disclosure of their health data.
Integrity	The impact of the loss of integrity will depend on the nature of the telemedicine/remote care application. For non-critical consultation applications the impact may not be as significant, but depending on the context, alteration of medical data could have high-impact consequences. Data subjects may encounter significant or even irreversible consequences from unauthorised alteration of health data (signals and statistics), which could even make it difficult for them to receive appropriate treatment.
Availability	Assessing the impact of loss of availability heavily depends on the context of the telemedicine/remote care application. This may range from low in the case of standard consultations for which alternative methods of communication can be used to very high in the case of emergency interventions of medical staff using the telemedicine platform.

ASSESSING RISK LIKELIHOOD

The table below describes how the main Cloud security threats may be relevant for the reference Cloud architecture and the specific use case. Healthcare organisations should use the information below when assessing the likelihood of a cybersecurity risk. It should however be noted that the descriptions below only refer to the described use case and additional factors related to the operational context of the healthcare organisation should be considered before determining the risk likelihood. Similarly the underlying telecommunications infrastructure-backbone would be a risk factor, however not in the scope of this assessment.

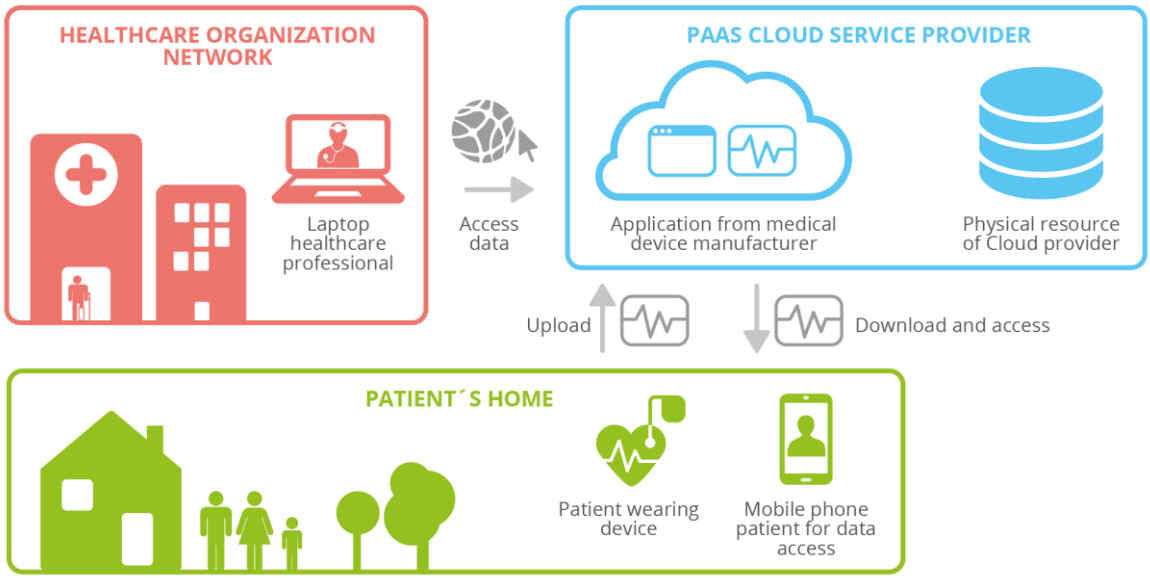
Threat	Description
Natural phenomena	Typically, in such use cases, the servers are located in data centres enforcing a suitable level of physical security requirements, which tends to reduce the respective risk likelihood. Such data centres usually obtain certificates that show that they are protected against fire, water, or earthquakes and the existence of such certificates should be factored into the risk likelihood assessment.
Supply chain failure	As the infrastructure is outsourced to Cloud providers the likelihood of this risk tends to be reduced. The failure of power supply or other Cloud service disruptions is less likely because the providers are specialised in maintaining their services. However, even big Cloud platforms are not entirely immune to outages of their Cloud infrastructure.
Human error	(Video)Conferencing tools are considered standard IT equipment which makes it more likely that users are familiar with this technology and the relevant interfaces. Especially during the pandemic situation, the adoption of and familiarisation with videoconferencing solutions has increased significantly. Still, the risk may be higher when medical staff are less familiar with or un-trained in the use of such tools.
Malicious actions	During the pandemic, many stakeholders have switched to remote conferencing and telemedicine, which in turn has led to such solutions becoming more attractive targets. Healthcare organisations also extended the use of teleconsultation. Potential attacks in this area might involve social engineering (e.g. phishing), theft, espionage, malware (e.g. ransomware), or denial of service attacks.
System failures	Videoconferencing technology has been developed and improved for a long time, resulting in well-established software solutions. Nevertheless, software failure might still happen with low likelihood since Cloud has enough redundancy.

4.3 USE CASE 3 – MEDICAL DEVICES

Medical device data is made available to different stakeholders using Cloud technology to enable remote patient monitoring e.g. for heart disease or diabetes patients. Medical device manufacturers also provide medical device monitoring using Cloud computing technology.

In this use case, we consider a medical device manufacturer that produces a device to measure certain patient data (e.g. a pacemaker measuring heartbeat). The device itself is not able to communicate over the internet. However, it can transfer measurements via Bluetooth to smartphones with an appropriate app from the device manufacturer. The app can then transfer the aggregated measurements for a month to a Cloud file storage provider and share this information with the treating doctor.

Figure 3: Cloud Architecture Model - Medical Device



OVERVIEW

Service Model	PaaS	**Deployment model**	Private Cloud
Healthcare organisation	The healthcare organisation offers its patients a medical device (e.g. pacemaker) that is connected to their mobile device. Healthcare professionals can access the measured data over the internet using their clients.		
Medical device manufacturer	The medical device manufacturer offers a Cloud service for patient measurements (e.g. measuring heartbeats) to healthcare organisations. The medical device manufacturer provides the application and the device and ensures the connection to the Cloud service provider through APIs for data transfer. It uses PaaS to securely develop and deploy the software, including sending emails with individualised links containing the uploaded aggregated measurements.		
Cloud service provider	The Cloud service provider provides the application platform, including application interfaces and the underlying Cloud infrastructure that includes network, servers, operating systems, and storage.		

DEFINITION OF PROCESSING OPERATION AND ITS CONTEXT

Personal data processed	Contact information (last and first name), health data (e.g. heartbeat) measurements
Processing Purpose	Provision of healthcare services (e.g. sharing heartbeat measurements)
Data Subject	Patients
Recipients of the Data	Medical professionals
Data Processor	PaaS Cloud service provider

ASSESSING CYBERSECURITY RISK IMPACT

When conducting a risk assessment for similar use cases, healthcare organisations should take into account the possible impact of a cybersecurity incident on confidentiality (e.g. data breach leading to exposed patient data), integrity (e.g. alteration of important patient data) or availability (e.g. timely access to patient data). This would allow the healthcare organisation to assign an appropriate quantitative or qualitative value to the risk impact depending on the specific risk assessment methodology used. While this specific use case only involves collection of patient data that is then subject to examination by medical staff, other use cases involving medical devices may include the device itself taking actions based on measurements, resulting in a drastically different risk profile. A brief description of factors to be considered for risk impact assessment is listed below:

Factor	Description
Confidentiality	Loss of confidentiality for similar use cases may cause data subjects to encounter significant adverse effects from unauthorised disclosure of their health data. Within the scope of the specific processing operation, the impact from loss of confidentiality is not necessarily considered critical since the disclosure of measurements such as heartbeats is usually not as severe as disclosing other health data. However if the data is exchanged in its entirety through unsecure means (i.e. email) poses a risk in itself. In a broader context, the impact of loss of confidentiality for use cases involving medical devices depends on the nature of the data involved in the operation.
Integrity	In the case of loss of integrity, data subjects may encounter significant or even irreversible consequences from unauthorized alteration of health data. For instance, doctors may prescribe inappropriate medication. This impact is heavily influenced by the overall treatment process; for instance, a doctor might notice sudden deviations from regular measurements and doctors usually explain treatment procedures or changes in medication via personal conversations, which might reveal the alteration of data. In the case of more automated processes or even processes where the device can even act based on the data, the impact of loss of integrity may be significantly higher.
Availability	The impact of loss of availability may range from moderate to critical depending on the frequency by which the measurements need to be made available to medical staff or even the nature of the measurements (e.g. when an anomaly in measurements may indicate a life threatening circumstance). The lack of data may affect the patient's health because unavailability affects intervention options.

ASSESSING RISK LIKELIHOOD

The table below describes how the main cloud security threats may be relevant for the reference cloud architecture and the specific use case. Healthcare organisations should use the information below when assessing the likelihood of a cybersecurity risk. It should however be noted that the descriptions below only refer to the described use case and additional factors related to the operational context of the healthcare organisation should be considered before determining the risk likelihood.

Threat	Description
Natural phenomena	Typically, in such use cases the servers are located in data centres enforcing a suitable level of physical security requirements, which tends to reduce the respective risk likelihood. Such data centres usually obtain certificates that show that they are protected against fire, water, or earthquakes and the existence of such certificates should be factored into the risk likelihood assessment.
Supply chain failure	As the infrastructure is outsourced to Cloud providers, the likelihood of this risk rends to be reduced. The failure of power supply or other Cloud service disruptions is less likely because the providers are specialised in maintaining their services. However, even big Cloud platforms are not entirely immune to outages of their Cloud infrastructure.
Human error	The medical devices need to be configured and require patches. The lack of patches or adequate configuration, procedures, or processing errors may leave the device vulnerable to cyberattacks.
Malicious actions	The system handles patients' private information, which might be interesting for malicious actors. Malicious attackers may also be internal actors who might have direct or indirect access to the Cloud services. Potential attacks in this area might involve theft, espionage, malware (e.g., ransomware), or denial of service attacks. On the other hand, Cloud service providers can have access to the knowledge of internal and external security experts, which allows them to enforce security measures more efficiently than proprietary data centres. These factors and especially the operational context of the healthcare organisation and the Cloud service provider should be assessed when determining the risk likelihood.
System failures	Medical devices undergo an extensive certification process that should impact occurrence probability positively. The software to access the health data may be subjected to failures, but security requirements are relatively high to ensure patient safety. Network and IT hardware failure may occur and depends heavily on the location. However, there is very low probability for system failures due to the multi tenancy and redundancy the Cloud services offer.

5. CLOUD SECURITY MEASURES

This section provides a set of guidelines for ensuring cybersecurity and data protection for the healthcare sector's Cloud customers procuring and eventually providing Cloud-based healthcare services. The security measures are based on common frameworks for Cloud security such as BSI C5 and ANSSI Cloud recommendations, but also the ongoing work on Cloud certification. This section contains the security measures with corresponding references to the good practices of ENISA's procurement guide and the use cases.

5.1 CLOUD SECURITY MEASURES AND GOOD PRACTICES

In general, the Cloud security measures, and the corresponding responsibility depend heavily on the chosen service and deployment model.

Each Cloud security measure entails:

- a reference to the good practices of the Procurement Guide (ENISA, 2020),
- a reference to the use case, for which the measure is applicable,
- an indication of the responsibility per use case and
- additional data protection considerations.

The last item relates to how each security measure eventually satisfies a potential data protection requirement and shows how through this measure acceptable implementation of the requirement is met. Some use cases require stronger data protection measures due to the criticality of the data and the evaluated risk. These enhancement considerations are attached to the Cloud security measures where applicable.

SM-01	Identify security and data protection requirements
Involve necessary stakeholders such as risk, legal, compliance, or IT department in the procurement process. Requirements solicitation should entail regulatory compliance. Investigate and identify requirements such as: • local legislation and pan-area legislation for cloud security, cybersecurity and data protection • internal requirements such as information security policies • legal requirements which apply to a specific healthcare product, for instance, countries enforce specific security and data protection requirements for electronic health records. • security and data protection requirements of the governmental Cloud service provider. Check and assess legal requirements for data protection, cybersecurity, and Cloud security. Reconcile legal requirements with the security controls of the Cloud service provider. In this case, it would be essential for the health care organisation to tag and assign data based on sensitivity levels, and ensuring that is provided to the CSPs so they can assign higher or lower levels of controls depending on the data. Request evidence from the Cloud provider such as certification from third-party auditors to ensure the Cloud provider's adherence to recognised standards. Ensure that responsibilities for ensuring compliance between the Cloud customer and Cloud service provider are identified and understood. Address security and privacy requirements in the service level agreement between the Cloud customer and the Cloud service provider. Require proof from the CSP for ensuring compliance with the requirements.	
Reference to Good Practice Procurement	GP 1. Involve the IT department in procurement

Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x	x	x
	Cloud Service Provider			
Additional data protection considerations		Preserve the right of data subjects taking into account: • the obligation to provide information on the ground for data processing; • data subject's consent for the processing • the right to access data • the right to data minimisation (only the information required) • the right to rectification and erasure Require data storage within the country of the HCO. Ensure privacy by design principles are followed both for the HCO and the CSP based on the service model followed. Cloud customer must ensure that data is securely transferred and verified at a safe location before the cloud provider could permanently delete the data. The cloud customer should be responsible for this timely data transfer and the contractual needs to allow for a proper transfer.		

SM-02	**Conduct a risk assessment and data protection impact assessment**			
Conduct a risk assessment according to national guidelines or following a well-known methodology (find some here[23]) to identify cybersecurity and data protection threats and risks for new Cloud services and evaluate the impact on the overall IT security risk Conduct a data protection impact assessment when procuring Cloud services (ENISA tool for evaluating the risk of personal data processing operation[24]) Ensure alignment with the healthcare organisation's risk appetite by identifying and implementing controls to mitigate identified risks to the organisation's risk acceptance level, by refraining from procuring the Cloud service or choosing another provider. Monitor the risk landscape continuously to be able to identify emerging risk or to enforce further controls.				
Reference to Good Practice Procurement		GP. 11 Conduct a risk assessment as part of the procurement process GP. 19 Conduct data protection impact assessment for new products and services		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x	x	x
	Cloud Service Provider			
Additional data protection considerations		none		

[23] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/business-process-integration/the-enisa-rm-ra-framework
[24] https://www.enisa.europa.eu/risk-level-tool/risk

SM-03	Establish processes for security and data protection incident management

Ensure that an incident response plan defines the actions to be taken after a security incident has occurred at the Cloud service provider. The Cloud service provider should have a process for handling security incidents according to European or national legislation.

Identify the responsibilities of Cloud customers and Cloud service providers in the case of a security or data protection incident.

Ensure that internal measures, processes, and roles are in place and aligned with the Cloud service provider's security provisions.

Test security incident processes in collaboration with the Cloud service provider and verify how a security incident can be reported to the Cloud service provider.

Request reports from the Cloud service provider for detected security incidents and the status monitoring of reported security incidents by the Cloud service provider.

Ensure SLA contains at least performance indicators of defined availability and capacity of the Cloud service, response and reaction times of the Cloud service provider's service organisation, notification of predefined maintenance or other planned downtime, and occurred security incidents either by default or on request.

Reference to Good Practice Procurement		GP 22. Develop incident response plans GP 23. Involve vendor/manufacturer in incident management		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x		x
	Cloud Service Provider	x	x	x
Additional data protection considerations		Ensure patients/customers are informed if their data has been subject to a security incident. Ensure legal obligations to notify are met. For Cloud customer: ensure the contact person at the Cloud service provider is reachable 24/7 and response is guaranteed within a predefined time.	Ensure patients/customers are informed if their data has been subject to a security incident. Ensure legal obligations to notify are met.	Ensure patients are informed if their data has been subjected to a security incident. Ensure legal obligations to notify are met. For Cloud customer: ensure the contact person at the Cloud service provider is reachable 24/7 and response is guaranteed within a predefined time.

SM-04	Ensure business continuity and disaster recovery

Ensure the Cloud provider notifies planned downtime several days in advance.

Define processes for business continuity and identify the Cloud service provider's and Cloud customer's responsibility in the event of a service disruption. Ensure the Cloud service provider has an effective business continuity management plan (based on best practices or national guidelines).

Test the business continuity process and ensure that key roles are familiar with their tasks.

Define and document procedures and responsibilities for critical operations that can damage assets stored in the Cloud computing environment.

Examples of the critical operations are:

- installation, changes, and deletion of virtualised devices such as servers, networks, and storage;
- termination procedures for Cloud service usage;
- backup and restoration.

Ensure monitoring of these operations by a supervisor.

Disaster recovery and data restore

Identify disaster recovery and data restore requirements of the healthcare organisation. Assess whether the Cloud service needs provision from two separate locations that give each other redundancy.

Ensure disaster recovery and restore processes of the Cloud service provider are aligned with these identified requirements.

Identify the emergency contact of the Cloud service provider.

Request a test protocol from the Cloud service provider that shows successful disaster recovery and data restore process testing.

Backup

Ensure adequate backup (i.e., offsite backup or a multi-Cloud approach) to ensure business continuity in case of Cloud service provider failure or data loss.

If the event backup is part of the Cloud service, define or identify backup requirements following information security policies and legal requirements (to ensure compliance).

Request information on the Cloud service provider's backup capabilities and verify that these meet backup requirements. Implement backup capabilities if the Cloud provider does not provide them, or the requirements are not met.

Reference to Good Practice Procurement		GP 6. Establish Business Continuity plans		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x	x	x
	Cloud Service Provider	x		
Additional data protection considerations		none		

SM-05	**Termination and secure data deletion**

The Cloud customer's asset stored on the Cloud service provider's premises should be removed, and returned if necessary, promptly upon termination of the contractual agreement or if data retention period is met. Proper permanent deletion of data upon customer's or data subjects is the full responsibility of the Cloud provider.

Data deletion

Ensure data is deleted according to recognised standards or techniques, meaning permanently and irretrievably deleted, and taking into account backup and log data.

Termination

Request a description of the termination process, disposal and return of Cloud customer's asset and reuse of resources from the Cloud service provider.

Ensure the description contains a list of all the assets and documents the schedule for the termination of service, which should occur promptly.

Reference to Good Practice Procurement				
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer			
	Cloud Service Provider	x	x	x
Additional data protection considerations		All necessary measures to ensure data deletion should be in place and documented in data retention policy (including technical means to support data stored in several systems). The policy should also include cases of data replication (storage in multiple sites) which would mean enabling tracing of the data to ensure complete deletion. Client-side encryption versus server-side encryption could be a solution to this[25].		

[25] https://www.enisa.europa.eu/publications/privacy-and-security-in-personal-data-clouds

SM-06	Auditing, logging and monitoring

Define or identify requirements for event logging (for instance, audit trails for patient to control access to their EHR, retention of logs) and verify if the Cloud service provider meets those requirements.

Determine and evaluate the adequacy of the Cloud service providers logging capabilities for privileged operations. Ensure privileged operations delegated to the Cloud service provider are logged, and the Cloud service provider provides corresponding log reports on request. Request documentation from the Cloud service provider of service monitoring capabilities and ensure the monitoring data is consistent with event logs and SLA terms.

Ensure that the Cloud service provider meets the agreed capacity requirements through continuous monitoring. Monitor and forecast the use of Cloud services to promptly communicate changes in capacity to the Cloud service provider and ensure quick adjustment.

Implement additional logging capabilities to close the gap between the Cloud service provider's logging capabilities and the Cloud customer's requirements.

Ensure data retention for log data follows legal requirements. Ensure log data is also deleted in the case of termination or change of provider.

Auditing the Cloud provider is a rather cumbersome task for the healthcare organisation to take over; auditing takes place at specific intervals to ensure compliance and certification maintenance.

Reference to Good Practice Procurement		GP 9. Allow auditing and logging		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x	x	x
	Cloud Service Provider			
Additional data protection considerations		none	none	none

SM-07	Implement vulnerability and patch management

Identify the scope of responsibility for technical vulnerability management and patch management. Determine and set up processes for vulnerability management and patch management in scope.

Request specifications of the cloud service provider's vulnerability and patch management practices that affect the Cloud service. The Cloud service provider should give evidence of regularly performed technical assessments such as penetration tests or vulnerability scans either by default or at the Cloud customers request. Conduct or request security testing in the event the cloud service provider cannot provide evidence, or the application has not been tested.

Reference to Good Practice Procurement		GP 2. Implement a vulnerability identification and management process GP 5. Establish testing policies		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x		x
	Cloud Service Provider	x	x	x
Additional data protection considerations		none	none	none

SM-08	Manage assets and classify information

Include information and assets stored in a Cloud environment in the asset inventory. Indicate where the data is stored, i.e. Cloud services. Asset changes should be monitored and recorded.

Classify information and data that will be stored or stored in a Cloud environment to meet security requirements.

Align change management process between the Cloud service provider and healthcare organisation. Ensure any change made by the Cloud service provider is taken into account in the internal change management process.

Identify the data protection levels for data confidentiality, integrity, and availability.

Reference to Good Practice Procurement		GP 28. Perform asset inventory and configuration management		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x	x	x
	Cloud Service Provider			
Additional data protection considerations		Information should be protected according to the risk assessment or the DP impact assessment.		

SM-09	Enable data encryption for data at rest and data in transit

Ensure data in the Cloud service provider's location is encrypted during the whole data life cycle (creation, storing, using, sharing, archiving, deleting).

Review the Cloud provider's encryption practices to ensure they meet the required encryption level, are compatible with other cryptographic protection, and meet regulatory requirements.

Ensure data transfer from and to the Cloud service for all incoming and outgoing connections is encrypted.

(note for the author: Encryption in transit is always a shared responsibility- the Cloud customer needs to take the appropriate measures to ensure that encryption will function properly (i.e. provider or patient using outdated browsers with known vulnerabilities in encryption protocols will result into breaking the encryption measures applied by the CSP).

Reference to Good Practice Procurement		GP 10. Encrypt sensitive personal data at rest and in transit		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x	x	x
	Cloud Service Provider	x	x	x
Additional data protection considerations		Ensure data at rest including backup and data-in transit is encrypted. Advise on client side encryption.	Ensure data-in transit is encrypted. Advise on client side encryption.	Ensure data at rest including backup and data-in transit is encrypted. Advise on client side encryption.

SM-10	Ensure security of encryption keys

Define security requirements for key management and ensure procedures for key management are implemented.

Identify cryptographic keys for each Cloud service and manage them according to defined requirements and procedures.

In the event the cloud service provider offers key management functionality, request documentation from the Cloud service provider on the type of keys used, specifications of key management covering procedures for each stage of the key lifecycle such as generating, changing/updating, string, retiring, retrieving and destroying.

Ensure keys are stored on certified devices (for example, hardware security modules), which ensure the level of protection for the key material.

Ensure segregation of duties is in place for the key management and is enforced by technical or organisational means.

Ensure a process for recovering encryption keys is in place.

Evaluate an encryption approach (provider- or client-managed key or hold- your-own-key) based on the risk analysis for your data and business. Where possible, use a client server-managed key.

Reference to Good Practice Procurement		GP 10. Encrypt sensitive personal data at rest and in transit		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x		x
	Cloud Service Provider	x	x	x
Additional data protection considerations		none	none	none

SM-11	Data portability and interoperability

Ensure all data is provided in industry-standard format upon request from the Cloud service provider.

Make sure the Cloud service provider uses standardised and secure network protocols for the import and export of the data to and from the Cloud service.

Interoperability

The Cloud service provider should use open and published API to support interoperability between components and applications.

Ensure the Cloud service provider uses an industry-recognised virtualisation platform and standard virtualisation formats to support interoperability.

Reference to Good Practice Procurement		-		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x	x	x
	Cloud Service Provider			
Additional data protection considerations		none	none	none

SM-12	Client and endpoint protection			
Identify all devices such as laptops, mobile devices, medical devices, etc. (endpoints) of your personnel connecting to the Cloud service. Ensure that the identified assets are included in the asset inventory. Define a security baseline for hardening the endpoints according to internal information policies and ensure device configuration meets the requirements during the whole lifecycle. For example, this could be achieved using a device management solution or regular assessments of the client's current state. Implement technical controls to meet security requirements. Use tools for facilitating endpoint security offered by the Cloud service provider.				
Reference to Good Practice Procurement		GP 28. Perform asset inventory and configuration management		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x	x	x
	Cloud Service Provider			
Additional data protection considerations		none	none	none

SM-13	Authentication and access control			
Ensure access policies specify security requirements for user access to data, application interfaces, systems, and the network or network components for each Cloud service. Ensure that access to the Cloud services is secured by strong authentication controls such as multi-factor authentication. Ensure a process for restoring authentication data is in place. Determine whether access to the Cloud service, Cloud service functions, and Cloud customer data can be restricted following the internal access policy.				
Reference to Good Practice Procurement		-		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x	x	x
	Cloud Service Provider			
Additional data protection considerations		Two-factor authentication should be mandatory for providers and recommended for patients	Two-factor authentication should be mandatory for providers and recommended for patients	Two-factor authentication should be mandatory for providers and recommended for patients

SM-14	Information security awareness, education and training

Establish a regular target group-oriented awareness and training programme for all internal (employees) and external actors (Cloud service providers), which deal with sensitive data such as electronic health records or medical diagnosis. Educate medical staff on what sort of security benefits CSPs provide in terms of risk reduction, protection of patients health data, etc. Realising that there are core benefits to outsourcing security where trust and security are intrinsic to the business. More general cybersecurity awareness around social engineering attacks and good cyber hygiene for medical staff/health care professionals (e.g not always using the same login and passwords or requiring two factor authentication by default) would all help alleviate common human error.

The target group consists of supervising managers, operational staff, IT personnel, and users such as medical practitioners, nurses, and patients. Take special care of customers/patients security that is being provided around their data for their peace of mind.

Cover Cloud-related procedures and standards, risks and risk management, risks affecting the system and network environment when using Cloud services, and legal/regulatory aspects. Best practices and documented guidelines are also recommended to support the final goal.

Reference to Good Practice Procurement		GP 21. Provide cybersecurity training on the organisation's security practices to staff and external consultants GP 27. Raise cybersecurity awareness among staff		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x	x	x
	Cloud Service Provider			
Additional data protection considerations		none	none	none

SM-15	Network Security

Ensure traffic between untrusted and trusted connections of network environments and virtual instances is restricted and monitored. This configuration should be reviewed on an annual basis. Implement security measures according to risks identified including the additional function required: Intrusion Protection System, anti DDoS solutions, WAF, CASB, ATP, Threat intelligence.

Request information on the security perimeter from the Cloud service provider. Ensure that all allowed services, protocols, ports, and compensating controls are documented.

Reference to Good Practice Procurement		GP 15. Determine network requirements GP 28. Perform asset inventory and configuration management		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer	x		
	Cloud Service Provider	x	x	x
Additional data protection considerations		Ensure the network is protected using a firewall on protection level, intrusion prevention and detection system. Ensure the network is protected against denial-of-service attacks.	none	none

SM-16	Review isolation between tenants			
Ensure the Cloud service provider applies appropriate segmentation for data, applications (physical and virtual), infrastructure, and network between different tenants to restrict one tenant's access to another tenant's resources. Request evidence from the Cloud service provider of established policies and procedures, isolation of critical assets, and/or sensitive data. Make sure to securely configure the provided Cloud infrastructure functionality in order to achieve the required segmentation.				
Reference to Good Practice Procurement		GP 14. Segregate your network GP 28. Perform asset inventory and configuration management		
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer			
	Cloud Service Provider	x	x	x
Additional data protection considerations		none	none	none

SM-17	Physical and environmental security			
Ensure that the Cloud service provider provides physical security controls to protect data centres and prevent unauthorized physical access. Controls include physical authentication mechanisms or electronic monitoring and alarm systems. Ensure that the Cloud service provider restricts its support staff's access to physical resources according to the need-to-know or least privileged principles. The Cloud service customer should request certifications that prove that the Cloud service provider's infrastructure is hosted in a secure data centre.				
Reference to Good Practice Procurement				
Application to Use Case		Use Case 1	Use Case 2	Use Case 3
		x	x	x
Responsibility	Cloud Customer			
	Cloud Service Provider	x	x	x
Additional data protection considerations		none	none	none

6. CONCLUSION

For a number of years healthcare organisations have been contemplating moving part of their ICT infrastructure and services to the Cloud. Over this period, a number of healthcare-specific solutions have been developed using a variety of service models and deployment models fit for purpose. The on-going pandemic has further highlighted the importance of certain healthcare services that could benefit significantly from a move to the Cloud. The potential improvements in availability, scalability and reliability of services such as telemedicine, wider deployment and use of EHR and medical devices for remote patient care come on top of the cybersecurity, economic and efficiency benefits Cloud services can bring to healthcare organisations.

Yet, the level of adoption of Cloud services in healthcare remains low and generally limited to administrative processes. A number of factors contribute to this, including lack of trust in Cloud services, lack of expertise, compliance requirements, particularly in relation to data protection, and more.

This report aims to help healthcare organisations in taking the next step towards further adoption of Cloud services. Built around three standard use cases of Cloud services in a healthcare context, this report highlights the main factors to be considered from a cybersecurity and data protection standpoint when assessing the relevant risks. The factors can be used in any risk assessment methodology that the healthcare organisations are currently using. Moreover, the report proposes a set of security measures for healthcare organisations to implement when planning their move to Cloud services. These measures cover both cybersecurity and data protection aspects and are linked to the procurement guidelines for healthcare organisations previously published by ENISA.

While this report is a step towards supporting healthcare organisations in taking the next step towards Cloud services it is not enough on its own. Healthcare organisations would require additional support, such as specific guidance from national and EU authorities, industry standards on Cloud security, especially in a healthcare context, clear guidelines from Data Protection Authorities on moving healthcare data to the Cloud and collaboration with Cloud service providers and medical device manufacturers to develop suitable Cloud solutions.

7. REFERENCES

AbuKhousa, E., Mohamed, N., and Al-Jaroodi, J., e-Health Cloud: Opportunities and Challenges, Future Internet, Vol. 4, 2012, pp. 621-645, doi: 10.3390/fi4030621

Agliari, E., Barra, A., Barra, O. A., Fachechi, A., Franceschi Vento, L. & Moretti M., Detecting cardiac pathologies via machine learning on heart-rate variability time series and related markers, Sci Rep 10, 8845, 2020, https://doi.org/10.1038/s41598-020-64083-4

Cloud Security Alliance, Top Threats to Cloud Computing – The Egregious 11, 2020.

Cavoukian, A., Fisher, A., Killen, S. et al., Remote home health care technologies: how to ensure privacy? Build it in: Privacy by Design, Identity in the Information Societey IDIS, Vol. 3, 2020, pp. 363–378, https://doi.org/10.1007/s12394-010-0054-y

Davenport, T., and Kalakota, R., The potential for artificial intelligence in healthcare, Future Healthcare Journal Vol. 6 No 2, 2019, pp. 94-98. doi: 10.7861/futurehosp.6-2-94

ENISA, Cloud Computing – Benefits, risks and recommendations for information security, 2012.

ENISA, Good Practice Guide for securely deploying Governmental Clouds, 2013.

ENISA, Procurement Guidelines for Cybersecurity in Hospitals, 2020.

ENISA, Security Framework for Governmental, 2015.

ENISA, Threat Landscape Report 2018, 2019.

IBM, X-Force Threat Intelligence Index, 2020, pp. 39.

IT Governance Privacy Team, EU General Data Protection Regulation – An Implementation and Compliance Guide, Third edition, It Governance Publishing, 2019.

Junaid Ahmad, B., Vinai, G., & Bilal, M., Cloud Computing with Machine Learning Could Help Us in the Early Diagnosis of Breast Cancer, 2015 Second International Conference on Advances in Computing and Communication Engineering, Dehradun, 2015, pp. 644-648, doi: 10.1109/ICACCE.2015.62

Leng, S., Tan, R.S., Chai, K.T.C. et al., The electronic stethoscope, BioMed Eng OnLine, Vol. 14, No 66, 2015, https://doi.org/10.1186/s12938-015-0056-y

NIST, The NIST Definition of Cloud Computing, Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, 2011.

NIST, NIST Cloud Computing Standards Roadmap, , Information Technology Laboratory National Institute of Standards and Technology, 2013. https://www.nist.gov/system/files/documents/itl/Cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

OWASP, OWASP Mobile Top 10, 2016

Sadhasivam, N., Balamurugan, R., and Pandi, M., Cancer Diagnosis Epigenomics Scientific Workflow Scheduling in the Cloud Computing Environment Using an Improved PSO Algorithm, Asian Pacific Journal of Cancer Prevention: APJCP, Vol. 19, No 1, 2018, pp. 243-246, doi:10.22034/APJCP.2018.19.1.243

Security Week, A Deep Dive Into Hyperjacking, February 2011.

Vacca, J. R., Security in the private Cloud, Taylor & Francis Group LLC, Boca Raton, 2017.

Ventsislav, V. and Rosen, I., Cloud-Based System for Real Time Medication Monitoring. In Proceedings of the 17th International Conference on Computer Systems and Technologies 2016 (CompSysTech '16), Association for Computing Machinery, New York , USA, 2016, pp. 151–158, doi : https://doi.org/10.1145/2983468.2983491

World Economic Forum, Understanding Systemic Cyber Risk, 2016, pp. 13.

A ANNEX: GENERAL PRACTICES

The tables presented below contain only the healthcare specific standards and guidelines. For a complete cybersecurity standards overview, you can reference to the ENISA Procurement Guide[26] of 2020.

STANDARD

Name - Description	Dimension (country)
ISA/IEC 62443 - A series of standards including technical reports to secure Industrial Automation and Control Systems (IACS).	Medical Devices (Health), Cybersecurity
NEN-7510 (NL) - This standard provides guidelines and principles for determining, setting and enforcing measures that an organisation in the healthcare sector must take to protect the information provision.	Cybersecurity (Netherlands)
NEN-7512 - Health informatics - Information security in healthcare - Requirements for trusted exchange of health information (NL) It applies to electronic communication in healthcare, between healthcare providers and healthcare institutions and with patients and clients, healthcare insurers, and other parties involved in healthcare.	Cybersecurity, (Netherlands)
NEN-7513 - Health informatics - Recording actions on electronic patient health records (NL)	Cybersecurity (Netherlands)
Hébergeurs de Données de Santé (HDS) - The Hébergeurs de Données de Santé (HDS) certification is required for entities such as Cloud service providers that host the personal health data governed by French laws and collected for delivering preventive, diagnostic, and other health services.	Cloud Security (France)

GUIDELINES AND FRAMEWORKS

Name	Description	Dimension (Country)
ANSSI SecNumCloud	The ANSSI SecNumCloud is the French pendant to the Criteria Catalogue C5, defining a baseline security level for Cloud computing. It is used by professional Cloud service providers, auditors, and Cloud customers. The criteria catalog was a collaboration work of Germany and France.	Cloud Security
Criteria Catalogue C5 – Federal Office for Information Security in Germany (BSI)	The Cloud computing compliance criteria catalog (C5) defines a baseline security level for Cloud computing. It is used by professional Cloud service providers, auditors, and Cloud customers.	Cloud Security
Cloud Security Alliance (CSA) – Cloud Controls Matrix	The CSA Cloud control matrix is a framework to ensure information security for Cloud computing providing 133 controls structured along 16 domains covering all key aspects of Cloud technology. It can be used as a tool to assess Cloud service providers and provides guidance.	Cloud Security
Cybersecurity Maturity Model Certification (CMMC)	The CMMC is a certification and compliance process developed by the Department of Defence. The certification aims at assessing the maturity level of fulfilling information security standards and best practices.	Cybersecurity

[26] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

Name	Description	Dimension (Country)
Health Information Trust Alliance (HITRUST)	HITRUST is a framework guiding the implementation of HIPPA requirements for healthcare providers. The HITRUST certification is a way to show compliance with HIPPA requirements to third parties.	Privacy / Cybersecurity
Principles and Practices for Medical Device Cybersecurity27	The principles and practices for medical device of the international medical device forum (IMDRF) cybersecurity have been designed to provide concrete recommendations to all responsible stakeholders on the general principles and best practices for medical device cybersecurity.	Cybersecurity Medical Devices
Guías CCN-STIC de Seguridad[28]	The CCN-STICH are instructions, guidelines, and recommendations of the Centro Criptológico Nacional, aiming at improving the maturity level of the organisation's information security.	Cybersecurity (Spain)
CCN-STIC-823 Seguridad en etornos Cloud[29]	The CCN-STICH-823 covers instructions, guidelines, and recommendations of the Centro Criptológico Nacional, focusing on Cloud services.	Cloud Security (Spain)
TRAFICOM guidelines	The Finnish transport and communication agency and national cybersecurity centre provide guidelines on information security.	Cybersecurity (Finland)
Digital security: Guidance of services and security[30]	The Finnish Ministry of finance provides guidelines for information security.	Cybersecurity (Finland)
National Cybersecurity Framework[31]	The Centro national de Cibersegurança provides a national cybersecurity framework.	Cybersecurity (Portugal)
Security Recommendations of Ministry of Health[32]	The Portuguese Ministry of health provides recommendations for ensuring cybersecurity.	Cybersecurity (Portugal)
Official eHealth DSI provider guidelines and policies[33]	The electronic health digital service infrastructure (eHDSI) describes a solution to support implementing EU-wide projects for the healthcare sector, focusing on cross-border healthcare data exchange. The digital service infrastructure (DSI) supports interoperable services across the EU.	Cybersecurity

[27] http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf
[28] https://www.ccn-cert.cni.es/guias.html
[29] https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud.html
[30] https://vm.fi/en/information-security-and-cybersecurity
[31] https://www.cncs.gov.pt/en/
[32] https://www.dgs.pt/directorate-general-of-health/structure-and-legal-framework.aspx
[33] https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+STARTING+TOOLKIT

B ANNEX: MAPPING OF SECURITY MEASURES

ID	Name Measure	Natural phenomena	Supply Chain Failure	Malicious Action	Human errors	System Failures
SM-01	Identify security and data protection requirements	x	x	x	x	x
SM-02	Conduct a risk assessment and data protection impact assessment	x	x	x	x	x
SM-03	Establish processes for security and data protection incident management					
SM-04	Ensure business continuity and disaster recovery	x	x			x
SM-05	Termination and secure data deletion		x			
SM-06	Auditing, logging and monitoring			x	x	
SM-07	Implement vulnerability and patch management			x		x
SM-08	Manage assets and classify information					
SM-09	Enable data encryption for data at rest and data in transit			x	x	
SM-10	Ensure security of encryption keys			x	x	
SM-11	Data portability and interoperability		x			
SM-12	Client and endpoint protection			x	x	
SM-13	Authentication and access control				x	
SM-14	Information security awareness, education and training				x	
SM-15	Network Security			x	x	x
SM-16	Review isolation between tenants			x		
SM-17	Physical and environmental security	x			x	x

ABOUT ENISA

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

ISBN: 978-92-9204-405-3
DOI: 10.2824/454966