D3.1

Specification of S-EHR mobile privacy and security conformance levels - V1

ABSTRACT

This report addresses the specification of Smart Electronic Health Record (S-EHR) privacy and security conformance levels. The security conformance levels comprise the constraints that a S-EHR mobile app and a S-EHR Cloud have to fulfil to be considered secure, reliable and compliant to privacy requirements. At first cyber-risks and derivation of targets and countermeasures are identified. Beyond that, the legal framework, existing methods and models in literature, as well as existing tools are analysed. Based on that, general methodology for the definition of the security conformance levels from the project's perspective is defined.

Delivery Date	August 26th 2020
Work Package	WP3
Task	T3.1
Dissemination Level	Public
Type of Deliverable	Report
Lead partner	FRAU

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826106

This document has been produced in the context of the InteropEHRate Project which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826106. All information provided in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose.

CONTRIBUTORS

	Name	Partner
Contributors	Francesco Torelli	ENG
Contributors	Lucie Keunen	A7
Contributors	Sofianna Menesidou	UBIT
Contributors	Katerina Polychronopoulos, Tima Otu Anwana	UniV
Reviewers	Stefano Dalmiani	FTGM
Reviewers	Thanos Kiourtis	UPRC

LOGTABLE

Version	Date	Change	Author	Partner
0.1	19-02-20	Definition of report structure	Salima Houta, Marcel Klötgen	FRAU
0.2	26-02-20	Review of report structure Definition of Conformance levels Comments	Francesco Torelli	ENG
0.3	14-03-20	Initial contents for all chapters	Salima Houta, Marcel Klötgen	FRAU
0.4	18-03-20	Update of introduction	Francesco Torelli	ENG
0.5	15-04-20	Review of other contributions List of security goals Classification of requirements with respect to security goals and with respect to obligatory levels Provided definition of conformance levels	Francesco Torelli	ENG
0.6	21-04-20	Draft version of chapters 4, 5,	Salima Houta,	FRAU

		6	Marcel Klötgen	
0.7	22-04-20	Revision and additions for chapters 2, 5, 7	Salima Houta, Marcel Klötgen	FRAU
0.8	27-04-20	Review of new contributions Contribution to Privacy and security requirements Contribution to Constraints Update of conformance levels	Francesco Torelli	ENG
0.9	27-04-20	Edited tables in chapter 5 according to common agreements, additions to chapter 7, common and editorial updates.	Salima Houta, Marcel Klötgen	FRAU
1.0	28-04-20	First internal review	Thanos Kiourtis	UPRC
1.1	28-04-20	Second internal review	Stefano Dalmiani	FTGM
1.2	20-07-20	Addressed reviewer's comments: Edited style of references. Chapter 2 has been merged with chapter 1. Edited tables in chapter 4.	Salima Houta, Marcel Klötgen, Sofianna Menesidou, Francesco Torelli, Tima Otu Anwana	FRAU UBIT ENG UNIVIE
1.3	23-07-20	Final consolidation of the deliverable	Salima Houta, Marcel Klötgen	FRAU
1.4	2020-07-23	Quality Check	Argyro Mavrogiorgou	UPRC
1.5	2020-08-05	Adaption of references	Marcel Klötgen	FRAU
Vfinal	2020.08.26	Final check and submission	Laura Pucci	ENG

ACRONYMS

Acronym	Term and definition
APPC	The Advanced Patient Privacy Consents Profile defines a structural representation of a privacy consent policy. The definition allows for privacy consent policies that can include individualized parts, based on the patient's choices or other circumstances.
APPKRI	APPKRI was funded by the Federal Ministry of Health and implemented by the Fraunhofer Institute for open communication systems (FOKUS). The aim of the project is to define a meta criteria catalogue for the description and evaluation of health apps.
BPPC	Basic Patient Privacy Consents (BPPC) provides a mechanism to record the patient privacy consent(s) and a method for Content Consumers to use to enforce the privacy consent appropriate to the use.
CEM	Common Criteria Evaluation Methodology: Common Criteria evaluations are performed on computer security products and systems. The evaluation serves to validate defined claims.
EECC	European Electronic Communication Codes: European Electronic Communications Code (EECC) is an EU directive, which regulates electronic communications networks and services
GDPR	General Data Protection Regulation: The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).
NISD	Network and Information System Security Directive: first piece of EU-wide legislation on cybersecurity.
OTT	over-the-top media services (OTT): OTT are streaming media services offered directly to viewers via the Internet.
OWASP ASVS	Open Web Application Security Project Application Verification Standard: OWASP ASVS is a standard for performing security verifications at the application level.
S-EHR	Smart Electronic Health Record: A S-EHR is able to import/share data from/with EHR/EMRs and with research centres, using short-range wireless D2D (device to device) communication or remote communication protocols. The S-EHR allows storing on a smart device the health data about a single citizen and produced by the citizen itself or by HCPs.
S-EHR app	The S-EHR app is an implementation of S-EHR, fulfilling the S-EHR conformance

	levels.
S-EHR Cloud	The S-EHR Cloud is an implementation of the SCS.
SCS	Secure cloud service, fulfilling the S-EHR conformance levels, is able to store on the cloud the data collected by S-EHRs, adopting the standard protocols defined by the project. A citizen may choose to use a S-EHR mobile app without using any S-EHR cloud. In this case, his/her health data will be accessible to health professionals by using the short-range D2D protocol or the EHR federation.
XSS	Cross-site scripting (XSS) is a type of computer security vulnerability. It is typically found in web applications.

TABLE OF CONTENT

LIST OF TABLES

1. INTRODUCTION

Mobile devices are now the most common means of accessing the Internet, while the explosive growth of the Internet as well as the increasing trends in using smart applications provides a fertile playground for attackers [NAGARJUN 2018]. For instance, according to the report "Vulnerabilities and Threats in Mobile Applications 2019", high-risk vulnerabilities were found in 38% of mobile applications for iOS and in 43% of Android applications in 2019. In addition, several studies indicate that online users increasingly rely on smart mobile devices for their everyday activities and needs, while there have been rapid advances of information management specifically in healthcare [ENISA 2018]. Moreover, the understanding of how the apps practically operate is often complex, due to their dynamic environment, reuse of software libraries and interconnection with different networks and systems, thus making it even more difficult to assess their privacy and security characteristics. Although few mobile application developers might maliciously oversee data protection obligations, in many cases poor data protection and security practices are due to lack of awareness, knowledge or understanding on how to practically organize for and engineer privacy and security requirements into their tools [ALAZAB 2020]. Last but not least, the processing of personal data through applications is regulated by the General Data Protection Regulation (EU) 679/2016 (GDPR) and the NIS Directive are mandatory challenges. From all the aforementioned reasons, we can understand that one of the greatest challenges for the mobile device ecosystem is security and privacy.

1.1. Scope of the document

This document defines the first version of the S-EHR privacy and security conformance levels. The latter represent privacy and security constraints that any S-EHR Mobile App and S-EHR Cloud service have to fulfil to be considered secure, reliable and compliant to the privacy requirements of InteropEHRate. The InteropEHRate open specification leaves the freedom to different developers to develop different kinds of S-EHR Mobile Apps and S-EHR Cloud services, but all of them have to fulfil the S-EHR privacy and security conformance levels.

In short, the goal of the present report is to provide a checklist for evaluating the security level of a S-EHR app or of a S-EHR Cloud service.

1.2. Intended audience

The target communities of this deliverable are all stakeholders who are interested in the development of S-EHR Mobile Apps and S-EHR Cloud services which are conformant to the InteropEHRate open specification.

1.3. Structure of the document

Section 2 outlines the legal framework and requirements with respect to security, privacy and data protection on the Smart-EHR (S-EHR) mobile application. The state of the art is presented in Section 3. Methods from the literature as well as existing criteria catalogues and solutions and providers are listed. Chapter 4 presents the Privacy and Security requirements from a project perspective taking into account the previous sections. The concept of conformance levels is described in Section 5 where the chosen dimensions and methods are discussed in detail.

1.4. Updates with respect to previous version (if any)

Not applicable (this is the first version).

2. LEGAL FRAMEWORK

2.1. Introduction

The S-EHR app is a mobile health application to the extent that the app processes data containing user's electronic health care records, which are regarded as special categories of data. The S-EHR app provides a variety of functionalities in relation to data processing, including storage, accessing, receiving, explicit sharing, emergency sharing and data sharing for research purposes. The full description of the app functionalities and features are found in deliverable 6.2 of the InteropEHRate project. Given the sensitive nature of health data and the many functionalities envisaged by the app, developers must consider the legitimate concerns about privacy, data protection and security.

2.2. Classification of S-EHR App

The Medical Devices Regulation (MDR) [MDR 2017] lays down rules concerning the market placement or putting into service of medical devices, medical device software and related accessories for human use. The Regulation applies to medical devices and accessories for medical devices. A software or application may be classified as a medical device when the manufacturer intends it for one or more of the following **specific medical purposes** in Article 2(1):

- Diagnosis, prevention, monitoring, prediction, prognosis treatment or alleviation of disease.
- Diagnosis, monitoring, treatment, alleviation or compensation for an injury or handicap.
- Investigation, modification or replacement of an anatomy or a physiological process.
- Control of conception (impregnation)

In addition, a "medical device is one which does not achieve its principal intended action by pharmacological, immunological or metabolic means in or on the human body, but which may be assisted in its function by such means"[MDR Article 2(1)].

Whilst not being itself a medical device, an application may be classified as an accessory for a medical device when it is intended by the manufacturer to be used together with medical device(s). An accessory for a medical device is intended to enable the medical device to be used in accordance with its intended purposes or to assist its medical functionality in accordance with its intended purposes [MDR Article 2(2)].

Based on the current state of functionalities, **the S-EHR app does not appear to fit within the definition of a medical device or an accessory.** The S-EHR app is a standalone software performing actions specifically limited to the storage, exchange, transfer, accessing and retrieval of medical data. The purposes of data processing in the app do not meet the specific medical purposes required by the Regulation. Furthermore, the S-EHR app is not an accessory for a medical device as it is not intended to enable the use or functionality of any specific medical device(s).

Based on the European Commission Guidelines [EC 2016] the S-EHR app may be broadly classified as an 'information system' and specifically classified as an 'electronic patient record system'. Information systems are intended to store, archive and transfer data, therefore information systems are not qualified as medical devices. Electronic patient records are information systems which store and transfer electronic patient records,

aiming to replace patient's paper files or store records on a single information system. The European Commission Guidelines explicitly state that software providing these limited functionalities do not constitute medical devices because Software must have a medical purpose on its own to be qualified as a medical device software [EC 2016]. Based on this assessment, the functionalities of the S-EHR app are analogous to electronic health records and thus do not satisfy the criteria for a medical device or an accessory. As such, the provisions of the Medical Devices Regulation do not appear to apply.

2.3. Privacy, Data Protection and Security

The Charter of Fundamental Rights of the European Union (The Charter) [EU 2012] sets out the fundamental rights protected by the European Union (EU). The Charter enshrines inalienable and universal rights designed to uphold the dignity and freedoms of individuals in the EU. These rights include the right to privacy and data protection. Article 7 of the Charter guarantees the right to the respect for private life, including communications that may occur digitally. Article 8 of the Charter enshrines the right to protection of personal data. This imposes the requirement that personal data be processed fairly for a specified purpose, based on the data subjects consent or another legal basis. Ensuring the security of online activities and services is essential towards giving effect to these fundamental rights [EDPS 2019].

The European Commission has enacted a series of Regulations and Directives, to strengthen individuals' fundamental rights in the digital age and unify rules in the digital single market. This document focuses on the legal framework regarding privacy, data protection and security requirements in relation to the development and use of the S-EHR app within the EU.

2.4. Personal Data Processed by Apps

Protection in relation to the processing of personal data is a fundamental right, to which the GDPR [GDPR 2016] gives effect by setting the legislative framework for personal data protection in the EU. The GDPR has binding effect in all Member States; however, some provisions allow Member States to enact additional national rules [GDPR Article 3]. The GDPR seeks to contribute towards the accomplishment of freedom, security and justice by protecting the rights of data subjects and ensuring the free flow of personal data within the EU [GDPR Article 1].

The provisions of the GDPR apply when personal data is processed. In terms of Article 4, personal data means "any information directly or indirectly relating to an identified or identifiable natural person" (data subject). Such information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person [GDPR Article 4(1)]. The GDPR does not apply to anonymised personal data because anonymisation irreversibly destroys any means of identifying the data subject.

In the context of mobile apps, personal data may be provided by the user or found on the user's device. Personal data further includes metadata related to the user's device and behaviour [ENISA 2020 (1)]. The S-EHR app seeks to process personal data and metadata about the citizen's contact information, identity, location data, health conditions and social and healthcare network.

2.4.1. Lawful Processing of Personal Data

In accordance with Article 8 of the Charter, the GDPR requires that personal data be processed for specified purposes, in a fair manner based on a lawful ground. The data protection principles, found in Article 5 GDPR are essential for the lawful processing of personal data. The core principles are as follows:

- **Lawfulness, fairness and transparency** [Article 5(1)(a)]: Personal data must be processed fairly, for a specified purpose and on a legitimate ground. Furthermore, data subjects must be provided with information and communication related to processing activities and the exercise of their rights under the GDPR [EDPB 2017 (1)].
- **Purpose limitation** [Article 5(1)(b)]**:** Mobile apps need to have a specific lawful purpose for processing personal data and the data subject must be informed of this purpose (this may be done through the privacy policy) [EDPB 2013].
- **Data Minimisation** [Article 5(1)(c)]**:** Processing of personal data is limited to what is necessary in relation to the purpose for which they are processed.
- **Accuracy** [Article 5(1)(d)]: Personal data must be accurate and kept up to date. Reasonable steps must be taken to ensure that inaccurate personal data is rectified.
- **Storage limitation** [Article 5(1)(e)]: Personal data may be stored (in a form which allows identification of data subject) only for a period that is necessary for the purpose of processing.
- **Integrity and confidentiality** [Article 5(1)(f)]**:** The processing of personal data requires appropriate security, technical or organisational measures to provide safeguards from loss, destruction or damage.

To lawfully process personal data the data controller must be able establish at least one "legal basis" found in Article 6 and 9 (for special categories of personal data). These legal bases are equivalent and not subject to any hierarchy. The GDPR defines processing as any operation, which is performed on personal data, whether or not by automated means [GDPR Article 4(1)]. Pursuant to GDPR's Article 6 (1), the processing of personal data is lawful if at least one of the following six circumstances are met:

(a) The data subject gives consent;
(b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) Processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) Processing is necessary for the purposes of a legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.

Article 9 (1) GDPR prohibits the processing of special categories of personal data such as health data unless one of ten conditions are met. Pursuant to Article 9(1) GDPR, the following conditions may be relevant to processing through the S-EHR app:

(a) The explicit consent of the data subject;

(b) To protect the vital interests of a data subject or of another natural person, where the data subject is incapable of giving consent;
(c) Processing relates to personal data which are manifestly made public by the data subject;
(d) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(e) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(f) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

2.4.2. Consent Requirement

The consent of users forms an important legal basis for processing in the S-EHR app. When consent forms the legal basis for processing, no further processing beyond what is covered by the original consent is possible unless further processing is justified by another legal basis (other than consent) [EDPB 2017 (2)].

To lawfully process health data as envisaged using the S-HER mobile app, the explicit and valid consent of patients must be obtained and accurate records of consent statements must be maintained. The GDPR outlines the following elements and **conditions required for valid consent**:

- **Specific consent** - consent must be given in relation to one or more specific, explicit and legitimate purposes determined by the data controller. The procedure for obtaining consent must allow data subjects the freedom to give consent for some processing operations/purposes and not for others [GDPR Recitals 32]. For example, data subjects should be allowed to consent to the storage of health data, but not to the exchange of that data with third parties. This means that that possibility of partial consent should be facilitated [EDPB 2017 (2)].
- **Freely Given consent -** consent must be freely given; this implies an actual choice for data subjects [GDPR Recitals 43].
- **Informed consent –** providing information to data subjects prior to obtaining their consent is essential to determine the validity of the consent given. In Article 12 – 14, the GDPR outlines the information that must be provided to data subjects prior to obtaining consent. This information includes the identity of the controllers, the purposes and the legal basis of processing based on the provisions of Article 6 (1) and 9 (1). Furthermore, data subjects must be informed about the type of data collected as well as possible risks in connection with processing and the safeguards to mitigate such risks. Data subjects must be informed of their rights under the GDPR, including the right to withdraw consent at any time [GDPR Article 7]. For a detailed list, see Article 13 (1) and (2) and Article 14 (1) and (2). This information must be included in the privacy policy of a mobile app (further discussed in section 3.6 of

this document). If the data controller fails to provide accessible, relevant information to data subjects, "consent will be an invalid basis for processing" [EDPB 2017 (2)].

- **Unambiguous indication of wishes –** consent requires a clear statement from the data subject or a clear affirmative act through an active motion or declaration.[GDPR Article 7]
- **Explicit consent –** based on Article 9 (2) (a) GDPR, explicit consent is required for the processing of personal health data. The term explicit means that data subjects must give an express statement of consent.[EDPB 2017 (2)]
- **Demonstrate consent –** the burden of proof rests on data controllers to demonstrate that data subjects have given consent to the processing operations. This imposes an obligation on data controllers to keep accurate records of consent statements [GDPR Article 7(1) and Recitals 42].

In terms of Article 7 (3), data subjects have the **right to withdraw consent** at any time and must be informed of this right. The controllers must ensure that consent can be withdrawn as easily as it is given [EDPB 2017 (2)]. This implies that when consent is obtained via electronic means for example through one mouse click, data subjects must, in practice, be able to withdraw the consent equally as easily [EDPB 2017 (2)]. If consent is withdrawn, all data processing operations previously based on valid consent that took place before the withdrawal remain lawful [GDPR Article 7(3)]. However, once consent is withdrawn the controller is obliged to stop the processing actions concerned, unless there is another lawful basis justifying continued processing [GDPR Article 7(3)]. Once the InteropEHRate tools are available for public use after the completion of the project, continued processing might be justified based on the 'vital interest of the data subject' [GDPR Article 9(2)(c)] in scenario 2, 'public interest in the area of public health'[Article 9(2)(i)] in scenario 1. If there is no other lawful basis justifying the processing of the data, the data must be deleted by the controller(s).

The specifics for consent in the S-EHR app are contained in deliverable 2.2 of the InteropEHRate project. The consent of users is required at various stages when accessing the app. Users will be required to consent to the S-EHR data management activities at the point of installation. At this stage consent is required for the purpose of storing and managing personal health data. The user's consent is further required for data sharing functionalities as the S-EHR app facilitates the exchange of data between citizens, healthcare practitioners and researchers.

2.5. Data Security

One of the key requirements of the GDPR is that personal data is processed in a manner which ensures appropriate security and respect for privacy. Data controllers and processors are required to implement appropriate technical and organisational measures to ensure the protection of personal data against unlawful processing, loss, destruction or damage [GDPR Article 32(2)]. When implementing such technical and organisational measures, data controllers and processors must consider at least the state of the state of the art, the costs of implementation, the nature, the scope, context and purpose of processing [GDPR Recitals 74].

Article 32 of the GDPR contains provisions governing the security of processing. In Article 32 (1) (a) and (d), the GDPR suggests some concrete security measures including the pseudonymisation and encryption of personal data. Article 32 (1) (d) requires the implementation of a regular testing process, to evaluate the effectiveness of technical and organisation measures. Article 32 (1) (b) and (c) GDPR establishes general goals of the implementation of technical and organisational measures. Such measures must ensure that processing systems and services enable confidentiality, provide the ability to restore access to personal data, and maintain a

process for evaluating system security. The GDPR requires adherence to approved relevant codes of conduct [GDPR Article 40] such as the EU Code of Conduct on Privacy for mobile Health Apps and a GDPR approved data protection certification mechanisms [GDPR Article 42]

To implement GDPR security requirements, app developers must comply with the principles of **privacy by design and default** [GDPR Article 25]**.** The privacy by design principle requires that privacy requirements be considered at the earliest stage of development by embedding processing activities with organisational and technical measures that fulfil GDPR principles [ENISA 2020 (1)]. This requires the continuous assessment of data protection risks and the implementation of effective mitigating measures including data minimisation [GDPR Article 25(2)]. Data minimisation is an important GDPR principle, which requires that "personal data be processed in a manner that is adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed" [GDPR Article 5(1)(c)].

The privacy by default principle is contained in Article 25 (2) of the GDPR. This principle places an obligation on data controllers to implement privacy default settings to ensure that only personal data which are necessary for each specific purpose of the processing are processed. Data controllers are further obliged that by default personal data not made publically accessible without the data subjects intervention. This requirement applies to personal data connected, all processing activities, storage periods and the accessibility.

A **data protection impact assessment (DPIA)** is "a process designed to describe the processing of personal data, access its necessity and proportionality" [EDPB 2017 (3)]. The DPIA seeks to identify and minimize data protection risks. Conducting a DPIA is mandatory for data controllers when processing is "likely to result in a high risk to the rights and freedoms of natural persons" [GDPR Article 35]. The GDPR requires a DPIA in events of processing on a large scale of special categories of personal data, including data related to health [GDPR Article 9(1)]. In the context of apps, the data controller(s) is usually the app provider(s), which in many cases may not be the app developers. However, the DPIA can be essential to app developers to investigate the risks of their tools and embed privacy and data protection requirements by design [ENISA 2020 (1)]. A DPIA assessment will be completed as part of WP7.

In accordance with Article 35 (7), the **DPIA shall contain the following:**

- A systematic description of the processing operations, the purpose of the processing and the legitimate interest pursued by the controllers;
- An assessment of the necessity and proportionality of the processing operations in relation to the purpose;
- An assessment of the risks to the rights and freedoms of data subjects;
- The measures envisaged to mitigate the risks, safeguards and security mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.

2.6. Privacy Policies

In order to comply with the above mentioned privacy, security and data protection requirements the S-EHR app must contain a privacy policy, which is under construction in the InteropEHRate project. A privacy policy or notice is a public document that explains how and why personal data is processed, applying data protection,

privacy and security principles [ENISA 2020 (1)]. The information contained in the privacy policy should be differentiated from other non-privacy related information such as contractual terms and general terms of use.

Where personal data is processed, data subjects must be provided with a privacy policy which meets the requirements outlined in Article 12, 13 and 14 of the GDPR. In accordance with Article 12, the privacy policy must be presented in written form either physically or electronically using clear and plain language. Information may be provided orally upon the request of a data subject. The privacy policy must be provided in a "concise, transparent, intelligible and easily accessible way" in a timely manner [GDPR Article 12(1)]. These provisions impose a requirement on app developers to include privacy policies into mobile applications. An average person should easily understand the contents of such policies and the scope and consequences of processing must be clearly explained. Furthermore, the privacy policy should be immediately apparent to the users, for example through a link, in a FAQs page, by way of contextual pop-ups or in an interactive digital context though a chatbot interface [EDPB 2017 (1)].

The GDPR further stipulates the information to be contained in the privacy policy. The duty to provide information is placed on data controllers and aims to ensure fair and transparent processing [GDPR Article 12]. This information is contained in Article 12, 13 and 14 of the GDPR and has been explained in **section 3.4.2** of this document.

In addition to the information requirements in Article 12, 13 and 14 GDPR, the privacy policy must inform data subjects on their rights found in Article 15 to 22 GDPR. Article 15 contains the right to access, allowing data subjects to obtain from the controller confirmation as to whether or not their personal data are being processed. Article 16 holds that the data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data". In terms of Article 17 Data subjects have the right to the erasure of their personal data without undue delay (the right to be forgotten). Article 18 gives data subjects the right to restrict data controllers from processing personal data. The right to data portability enshrined in Article 20 ensures the free flow of personal data in the EU. The GDPR gives data subjects the right to object to the processing of their personal data at any time. Data subject's must be informed of this right, clearly and separated from other information at the time of first communication. Finally, Under Article 22 (1) GDPR, data subjects have the "right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects him or her". Data subjects must be informed about the existence of automated decision making including profiling.

2.7. Electronic Identification and Trust Services

The eIDAS Regulation establishes the legal structure for the use of electronic identification means and trust services (i.e. electronic signatures, seals, time stamps, registered electronic delivery and website authentication) throughout the EU. The Regulation aims to improve trust in the online environment by providing a common foundation for secure electronic interactions and ensuring an adequate level of security of electronic identification means and trust services [eIDAS Article 1]. This Regulation is applicable as the S-EHR app envisages the use of electronic signatures and timestamps as authentication mechanisms.

2.7.1. Electronic Signatures

The eIDAS Regulation identifies **three types of e-signatures:**

1. Basic e-Signatures

This refers to any kind of signature made by a natural person in an online environment that manifests the intention of the signatory to be bound by the contents of the signed document. In practice, this could be clicking a button or checking a box [eIDAS Article 3(10)].

2. Advanced e-Signatures

This refers to an eSignature that meets the requirements set out in Article 26. In terms of Article 26, an advanced eSignature must be uniquely linked to the signatory and capable of identifying the signatory [eIDAS Article 26(a)(b)]. Furthermore, the eSignature must be created using electronic signature creation data that the signatory can use under his sole control with a high level of confidence [eIDAS Article 26(c)]. Finally, the eSignature must be linked to the data in such a way that any subsequent change in the data is detectable [eIDAS Article 26(d)]. Article 26 requires the unique identity, sole control and integrity of the signed document to assure secure and reliable authentication of the signatory's identity in the online environment.

3. Qualified e-Signatures

According to Article 3(12), qualified electronic signature means an "advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures". An electronic signature creation device is a "configured software or hardware used to create an electronic signature"[eIDAS Article 3(23)]. The Regulation sets out strict requirements for the qualified electronic signature creation devices [eIDAS Article 29]. These devices shall adopt technical and procedural means to ensure that:

(a) The confidentiality of the electronic signature creation data used for electronic signatures is reasonably assured;
(b) The electronic signature creation data used for electronic signature creation can practically occur only once;
(c) The electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery;
(d) The electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others [Annex II].

In practice, the use of qualified electronic signatures and corresponding qualified certificates invokes an additional layer of assurance and trust that results in a special legal effect recognised by the courts in the EU. Qualified e-Signatures and corresponding qualifies e-certificates [Annex I] ensure data integrity, data security and the secure identification of the signatory. Article 25 of the eIDAS Regulation affirms the admissibility of eSignatures as evidence in legal proceedings. This Article holds that eSignatures cannot be denied legal effect solely because "it is in an electronic form or does not meet the requirements for a qualified electronic signature". Deliverable 2.2 of the InteropEHRate project contains further information regarding the use of e-signatures in the S-EHR app.

2.7.2. Timestamps

An electronic timestamp is "data in electronic form, which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time" [eIDAS Article 3(33)]. The eIDAS Regulation recognises qualified electronic timestamps, which meet following the three requirements set out in Article 42:

(a) The electronic timestamp binds the data to the date and time in such as way that the possibility of the data being changed is reasonably eliminated, ensuring data integrity;
(b) It is based on an accurate time sourced linked to Coordinated Universal Time (i.e. the clock used for time stamping is correctly synchronised with UTC);
(c) It is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

Data stamped using qualified electronic timestamps enjoys the legal presumption of accuracy and integrity throughout the EU. The integrity and security of the stamped data is further ensured via the advanced electronic signature on the timestamp, which guarantees that any alterations to the time stamped data can be detected [ENISA 2016].

2.8. Data Roaming

The S-EHR app envisages the cross border exchange of medical health data. For example, a patient visiting a foreign EU state will be able to use the S-EHR app to exchange his medical data with a foreign healthcare practitioner. In such scenarios, it is important to consider EU Regulation No 531/2012 [Roaming Regulation, 2012]. The Regulation focuses on the roaming charges within the Union when users utilise telephone and data services outside of network operators Member States. The Roaming Regulation also manages wholesale rates which networks can charge to each other to allow their subscribers access to each other's networks [RR 2012].

In 2017 the 'roam like at home' rules entered into force putting an end to roaming chargers. When travelling through the EU the cost of calls, SMS (to any EU number) and data usage are included in domestic bundles with no additional charges [EC 2020]. National telecom regulators are responsible for enforcing the roam like home rule [EC 2020]. Concerning wholesale roaming markets, the European Parliament and Council established the maximum price that operators have to pay each other for the use of networks when their customers travel in the EU. From 1 January 2020 till 1 January 2021, the wholesale price is set at EUR 3, 50 per gigabyte [RR 2017].

3. STATE OF THE ART

This chapter first lists some examples from the literature. Subsequently, service providers and existing frameworks / criteria catalogues are presented.

3.1. Literature review

The table below (Table 1) lists existing approaches described in scientific literature.

	Approach
[Sutton 2014]	The Patent includes a method, a mobile device, and a distributed security system (e.g cloud) that is utilized to enforce security on mobile devices which are coupled to external networks. The solution is platform independent and prevents malicious applications from running on a mobile device.
[Alenezi 2020]	The researchers used a hybrid method from Fuzzy AHP-TOPSIS (Analytical Hierarchy Process Technology for Order Preference by Similarity Ideal Solution) to evaluate the security design tactics and their attributes. The efficiency of this approach has been tested in a real-time web application. "A security tactic is a design concept that addresses a security problem at the architectural design level" The authors distinguish between three main categories of security tactics ● Availability based tactics (Fault Detection, Recovery Preparation and Recovery, …), ● Testability based tactics (Internal Monitoring, …) ● Usability based (Support User Initiative) tactics.
[Sönmez 2019]	OWASP is a non profit organization which produces standards, articles, tools, forum information related to web application security for architects, developers, analysts, and researchers. It provides a long list of security requirements; however, it does not provide an easy way to associate design features, environment properties, or technologies to these long lists of security requirements. The Open Web Application Security Project Application Verification Standard (OWASP ASVS) V.3. is commonly used for web application security evaluation and the security requirements determination. It consists of a total 182 security requirements grouped under the following 19 topics: architecture design and threat modelling, authentication verification requirements, session management verification requirements, access control verification requirement malicious input handling verification requirements, output

	encoding/escaping, cryptography at rest, error handling and logging, data protection, communications, HTTP security configuration, security configuration verification requirements, malicious controls, internal security verification requirement, business logic, file and resources, mobile, web services, and configuration.
[Bialas 2019]	The paper looks at the Common Criteria Evaluation Methodology (CEM), particularly its part related to vulnerability assessment. A structuring of the vulnerability assessment process on the basis of ontologies is proposed in order to make automation in the assessment possible. A tool based on this ontology should help to automatically identify security gaps.

Table 1 - Examples from literature

3.2. Existing solutions

This chapter includes existing open and commercial solutions as well as services. The table below (Table 2) lists existing service providers.

	Scope
Nodes Agency Germany GmbH	Nodes Agency Germany GmbH has developed a five-step method to help companies make their applications GDPR-compliant. The steps are: ● Check the data protection of the user interface (giving consent, continuously explanations for the user without impairing the user-friendliness) ● data and system mapping (different subsystems and integrations on which the data is stored and processed are described/mapped → data journey which describes the data usage) ● security check (security check and rate) ● contracts and accounts (keep control of contracts and billing with all suppliers and subcontractors, …) ● process recommendation (report that assesses a company's compliance across multiple touchpoints, for example it provides information on how users can get their data back, delete it, …)
Appicaptor - Test tool for app security of the Fraunhofer Institute for Secure Information Technology SIT	Appicaptor creates an individual test report for companies for every app and every operating system. These management reports are understandable even for people without deep IT security knowledge. The system can be configured individually. Test criteria can thus be adapted to the specific security guidelines of your own company. The analysis runs automatically. The system issues a warning if security gaps are found or if unsafe data is used. Since apps are revised regularly and

	new insights into vulnerabilities and implementation errors arise again and again, Appicaptor regularly repeats the tests and thus always evaluates the security properties based on the latest technical knowledge. Services: ● Carrying out app tests with cyclical updating of the respective app security assessment ● Recommended use of safe apps depending on their functionality and security requirements ● Concepts for the safe use of mobile devices (holistic mobile device management) ● Technical advice and IT security policy creation and testing ● Creation of app recommendation lists (blacklist / whitelist) ● Support in the development of secure apps ● Automated basic tests and compliance checks ● In-depth manual vulnerability analysis of apps ● Expert tests of app binaries and app source code audits ● Development of concepts, procedures and tools for IT security testing of mobile services and devices

Table 2 - Service providers

The table below (Table 3) lists existing open/commercial criteria catalogues.

	Scope
APPKRI (BMG)	https://ehealth-services.fokus.fraunhofer.de/BMG-APPS/ APPKRI was funded by the Federal Ministry of Health and implemented by the Fraunhofer Institute for open communication systems FOKUS. The aim of the project is to define a meta criteria catalogue for the description and evaluation of health apps. With this catalogue, health apps can be compared, evaluated and good applications recommended. Which requirements health apps should meet and which aspects are important will vary depending on the perspective of the examiner, but also depending on the user group under consideration, indication, application situation, objective, etc. Possible categories are user friendliness, data protection, reliability.
Guidelines on assessing Digital	The European Union Agency for Network and Information Security

Service Providers (DSP) and Operators of Essential Services (OES) compliance to the Network and Information system Security Directive (NISD) security requirements	(ENISA), a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens, has defined Guidelines on assessing DSP and OES compliance to the NISD security requirements. In order to have a common level of information security within the European Union (EU) network and information systems, a common set of baseline security requirements to ensure a minimum level of harmonized security measures across the EU is adopted. The parameters for Information Security audits and self-assessment / management are proposed within this Guideline.

Table 3 - Open/commercial criteria catalogues

3.3. Conclusion

Solutions for enforcing security requirements on mobile applications play a major role. The references listed above only show a selection of methods, service providers and frameworks that deal with this topic.

In addition to our specific project requirements, we also take into account the security requirements defined in OWASP (e.g. error handling and logging, data protection, cryptography) when defining our security goals and technical measures.

For further refinement of the levels and the definition of an assessment tool in version two of the document (31 Mar 2021), NISD security requirements and the associated guideline are taken into account in the sense of EU-wide harmonization.

4. PRIVACY AND SECURITY REQUIREMENTS

4.1. Personal Data

Privacy and protection regarding a citizen's personal data is ensured by law. With InteropEHRate, personal data is considered to contain (see report [D2.2]):

- information and knowledge about a citizen's identity and demographics
- information and knowledge about a citizen's health condition and history
- information and knowledge about a citizen's social and healthcare network
- information and knowledge about a citizen's location

In this context, information and knowledge consists of readable data and implicitly corresponding metadata. Metadata are an equally important part of information and knowledge and must be protected as well.

4.2. Security requirements

The use and distribution and ultimately the success of a mobile application that handles sensitive information is largely based on its trustworthiness and how it handles and addresses specific security goals. A list of security goals has been identified from the analysis described in the previous section.

The identified security goals can be achieved by ensuring several technical measures according to the following table.

Security Goals	Description	Possible Technical Measures
Confidentiality & Access Control	Assure that data are not accessed by not authorized people. Assure that the Citizen is in control of authorizations and consents.	- Data Storage Encryption - Transport Encryption - identity management - authentication management - authorization management - consent management - Policy Enforcement - physical security
Integrity & Authenticity	Avoid that data are accidentally or fraudulently corrupted or altered. Avoid that data are lost.	- Data Minimization - Qualified Digital Signatures - Timestamps - Certification of Software & Vendor - Verification of Digital Signatures - Backup of information - use of checksums for data transfer - Data Correcting Codes
Availability	Prevent unauthorised withholding of information or resources.	- Availability of information - High availability of storage systems - Prohibition of Data Erasure

		- Physical Protection - Computer Redundancies
Traceability & Non-Repudiation	Track the origin (source and author) of data. Assure that an author cannot successfully dispute its authorship or the validity of an associated contract.	- Auditing of Interactions - Confirmation Procedures (handshaking) - Session-Management - Data Provenance Tracking - Data Lineage - Validity through technical verification of transactions - Legal Certainty through verification of Digital Signatures

Table 4 - Possible Technical Measures for Security Goals

Table 5 explains the currently envisioned technical measures, which are mapped to (security) user requirements implying that measure and defined by report [D2.2].

The security goals must be implemented by technical measures that meet the state of the art. Each implementation can therefore be replaced with a more suitable or better one, as long as the same security goals are still achieved. For instance, according to [NIST 2020], the latest NIST recommendation for cryptographic algorithms, along with their associated key lengths, may become more vulnerable to successful attacks, requiring a transition to stronger algorithms or longer key lengths over time. Security strength is a number associated with the amount of work (i.e., the number of operations) that is required to break a cryptographic algorithm or system. In [NIST 2020], the security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256}. A projected time frame for applying cryptographic protection at a minimum acceptable security strength is at least 128 bits in 2031 and beyond. In addition, the estimated, comparable, maximum-security strengths for the approved symmetric block cipher and asymmetric-key algorithms and key lengths are AES-256, 15360-bit RSA, SHA-512 or SHA3-512, that corresponds to security strength 256. The security and technical measures are separated in two parts a) the first is based on the ENISA's Minimum Security Measures for Operators of Essentials Services [ENISA 2020 (2)] and the second on the main individual rights of the GDPR.

Security & Technical Measures			Protocols	User Requirement (see report [D2.2])	Implementation Decisions which provide minimum guarantees	Applies to S-EHR App	Applies to S-EHR Cloud
ENISA's **Security Measures**	Logging / Information system security audit	Auditing and Provenance Tracking of health data	D2D	#4: Auditing health data modification for Citizen on S-EHR; #64: Consultation of auditing health data modification for Citizen on S-EHR; #69: Non repudiable data provenance tracking; #76: Auditing health data sharing for Citizen on S-EHR; #77: Consultation of auditing health data sharing for Citizen on S-EHR	Any process upon data-interaction **SHOULD** be logged for transparency and auditing purposes.	Yes Satisfied by **D2D, R2D and R2D** protocol specifications Logs **CAN** be tracked in blockchain for a formal audit-trail	No

			R2D	#101: Auditing of HCPs that gained access for emergency reasons to Citizen's health data; #102: Auditing of changes to health data stored in the S-EHR Cloud; #105: Auditing of HCPs that gained access to the Medical Images; #137: Auditing of Organisations that gained access to health data for emergency reasons; #140: Auditing of citizens that gained access to their health data; #149: Citizen's			Yes (Native functionality of the cloud provider) Logs **CAN** be tracked in for a formal audit-trail

				consultation on S-EHR of S-EHR Cloud auditing data;			
			RDS	#93: Auditing of actions requested to IRS; #158: Logging of unsupported conversions and translations			No
	Information system security incident response	Backup of Information	R2D	#97: Activation of automatic backup of S-EHR content on selected S-EHR Cloud	*no specific mechanism has been identified*	Yes Satisfied by the **R2D** protocol specification	No
	Authentication and identification		D2D	#2: D2D Visualization of Healthcare organization to the Citizen; #17: D2D Identification and Authentication of the citizen from HCP; #23: D2D Visualization	The guarantee of an identity with non-repudiation guarantees **SHALL** be supported by one of two mechanisms: (a) Standalone mechanism: By presenting an eIDAS compliant Certificate	Yes Regarding mechanism (a), the developer/application-provider **SHALL** trust the European Trust Lists i.e. no additional signalling is required since this guarantee is satisfied by the **D2D** protocol.	No

			of Citizen identity to HCP; #75: D2D Visualization of Citizen identity to HCP (using certificate); #78: Enabling of Citizen identification from S-EHR (with CA); #79: Enabling of HCP identification from HCP app (with CA); #80: Enabling of healthcare organization identification from HCP app (withCA)	issued by a Certificate Authority that belongs to the European Trust Lists (ETLs) (b) Through additional signalling: By implementing the authentication signalling with a CEF-compliant eIDAS node (in potential inter-country or intra-country scenarios). In the first case the mathematical proof of the identity is locally computed, while in the latter case the eIDAS node acts as an authoritative proxy for the identity-proof (in the latter case the identity is accompanied		
		R2D	#138: Legal identification and authenticati on of qualified HCPs; #134: Citizen's access to		Yes Regarding mechanism (b), all required signalling is satisfied by the **R2D** protocols.	No **For Citizens** (Citizen interacti on with the cloud does not

			emergency token; #139: Legal identification and authentication of qualified Healthcare organisations; #143: HCP' access to Citizen identity by means of Citizen's token;	by a set of attributes that are guaranteed regarding their integrity and authenticity by the Proxy).		require the extraction of an eIDAS-compliant identity; but only an application specific user-identifier) Yes **For Health Organization Members** since they have to prove their identity (with one of the two mechanisms) prior to interacting with the stored data.

			RDS	#150: Identification and authorisation of organisations and researchers accessing to IRS		Yes Satisfied by the RDS protocol specification	No
	Access rights	Authorization & Policy Enforcement	D2D	#32: Implicit application of default S-EHR access permissions for D2D; #67: D2D authorization to download and upload S-EHR data from HCP App;	*no specific mechanism has been identified*	Yes Satisfied by D2D, R2D and R2D protocol specifications	No
			R2D	#99: HCP's access to health data of an identified citizen for emergency reasons; 104: HCP's access to Citizen's medical images for emergency reasons;	Any access request to cloud-resources (i.e. stored encrypted medical data) **SHALL** be authorized with a formal Access Control Mechanism. Indicative Access Control Mechanisms		Yes Existing InteropEHRate authorization engine can be used to formulate access control rules and

				#144: Authorisation to the healthcare team for emergency	include: (a) Access Control Lists; (b) Mandatory Access Control engines (a.k.a. MAC engines); (c) Discretionary Access Control engines (a.k.a. DAC engines); (d) Role-Based-Access-Control engines (a.k.a. RBAC engines); (e) Attribute-Based-Access-Control engines (a.k.a. ABAC) The adopter SHALL use one of these engines since they are functionally equivalent (they have significant differences in scaling, modelling overhead etc). For the sake of reference implementation,		evaluate any request towards stored data.
			RDS	#150: Identification and authorisation of organisations and researchers accessing to IRS			No

					InteropEHRateships with an ABAC engine that authorizes any request.		
	Cryptography	Data Storage Encryption	D2D	#70: Integrity of medical information	**Data-at-rest SHOULD** be symmetrically encrypted using a military-grade NIST-compliant algorithm (e.g. AES with 256bit key) Symmetric-Encryption Key (that is used for data-at-rest) **SHOULD** be stored and retrieved by a local Keystore (password-protected or biometric protected)	Yes It is used to encrypt medical data Android and iOS are providing libraries for local Keystore implementation	Yes it is used in the frame of Encrypted File System and based on confidential cloud computing (e.g. TEE)
			R2D	#70: Integrity of medical information; #103: Storing Citizen's Medical Images in the S-EHR Cloud			
			RDS	#70: Integrity of medical information			No
		Transport Encryption	D2D	#70: Integrity of medical information	Transport-level encryption **SHALL** be used e.g. TLS v1.2 which incorporates both secure-	Yes Satisfied by the D2D, R2D protocol and RDS specifications	No
			R2D	#70: Integrity of medical			Yes Satisfied by the

				information; #135: Encryption of S-EHR content exchanged with S-EHR Cloud.; #136: Encryption of health data written by HCP on S-EHR Cloud.	key-exchange and strong network-level encryption (e.g. Diffie-Hellman key exchange)		R2D protocol specifications
			RDS	#70: Integrity of medical information			No
		Integrity of medical information	D2D R2D RDS	#70: Integrity of medical information	Medical information **SHOULD** be stored and transferred digitally signed (e.g. along with the hashed part of the information) using a military-grade NIST-compliant algorithm (e.g. SHA3-512 and RSA)	Yes (see report [D3.5]) **For data in transit:** Satisfied by the D2D, R2D and RDS protocol specifications	Yes (see report [D3.5]) **For data in transit:** Satisfied by the D2D, R2D and RDS protocol specifications
		Privacy of the Citizen	RDS	#91: Automatic		Yes Satisfied by the **RDS**	No

				anonymization and sharing of citizen's health data for research; #130: Pseudoidentity restricted to single research protocol.		protocol specification	
	Physical and environmental security		D2D R2D RDS	#70: Integrity of medical information	*no specific mechanism has been identified*	No The citizen should protect his personal mobile device.	Yes The cloud provider **SHOULD** attest his/her cloud infrastructure. (Formal Attestation processes are emerging)
Data sovereignty & **GDPR**	The right to be informed; The right to object The right to restrict Processing	Consent Management	D2D	#10: Confirmation to enable the S-EHR data management; #11: Consultation on HCP app	Any process upon the citizen's data (e.g. store, access, transfer, update etc.) **SHALL** first be confirmed (or	Yes Satisfied by the D2D, R2D and RDS protocol specifications	No

				of consent by Citizen for temporary S-EHR access; #13: D2D consent by the Citizen for temporary S-EHR access to Healthcare organization; #19: D2D Access consent to healthcare organization by Citizen; #22: D2D Request of consent from HCP for download and storage of data from S-EHR and upload new data to S-EHR; #68: Consent to store Citizen's data	rejected) by the citizen and follow the data minimization rule according to the purpose of the processing. The purpose of the consent **SHALL** specifically be stated to restrict the process.		
			R2D	#97: Activation of automatic backup of S-EHR content on selected S-EHR Cloud;			Yes Satisfied by the R2D protocol

				#98: Sharing of health data with qualified HCPs for emergency by means of S-EHR Cloud			specification
			RDS	#86: Digitally signature by Reference Research Centre of Citizen's consent; #87: Citizen's digital signature of consent to share health data for a given study; #88: Citizen's digital revocation of consent to share health data for a given study; #107: Citizen's consent to be part of InteropEHRate Open Research Network; #109: Citizen's			No

				withdrawing from research network; #126: Citizen's consent to share health data for a research protocol; #128: Reception and storage of consent, digitally signed from research organisation, on Citizen's S-EHR; #129: Signed consent refers to the research protocol accepted by the patient.;			
	The right of access		R2D	#18: R2D import of (portion of) Laboratory result from national health care system on S-EHR; #20: R2D import of (portion of)	The Citizen **SHALL** be able to access his/her medical information stored on the S-EHR Cloud. The Health Organization	Yes Satisfied by the R2D protocol specification	Yes Satisfied by the R2D protocol specification

			Hospital discharge reports from national health care system on S-EHR; #21: R2D import of (portion of) health data from all national health care systems on S-EHR; #37: R2D import of (portion of) Medical images and reports from national health care system on S-EHR; #74: R2D import of (portion of) Patient Summary from national health care system on S-EHR (with security); #98: Sharing of health data with qualified	Members **SHALL** be able to access citizen's data stored on the cloud on emergency situations, through an emergency token.		

			HCPs for emergency by means of S-EHR Cloud; #104: HCP's access to Citizen's medical images for emergency reasons; #133: Automatic download of health records from S-EHR Cloud to S-EHR			
	The right to erasure	D2D	#13: D2D consent by the Citizen for temporary S-EHR access to Healthcare organization	The designed applications **SHALL** provide the relevant functionality considering the permissions and ownership of data using the implemented access management mechanisms.	Yes The app **SHALL** provide functionality to the user to partially or completely erase his/her personal or sensitive data.	Yes The app **SHALL** provide functionality to the user to partially or completely erase his/her personal or sensitive data from the EHR cloud.
		R2D	#102: Auditing of changes to health data stored in the S-EHR Cloud;			
		RDS	#109: Citizen's withdrawing from research			

			network			
	The right to rectification	D2D R2D RDS	#94: Patient Summary consultation on HCP App (with citizen update); #95: Update from the patient of personal health information	The mobile applications **SHALL** provide the ability to correct the medical information with auditing functionality enabled.	Yes The app **SHALL** provide functionality to the user to amend his/her personal or sensitive	No
	The right to data portability	D2D	#16: D2D download on HCP App from S-EHR of initial data set;	The designed applications **SHALL** provide the specification to transfer medical information among different devices.	Yes Satisfied by the D2D R2D and RDS protocol specifications	No
		R2D	#18: R2D import of (portion of) Laboratory result from national health care system on S-EHR; #20: R2D import of (portion of) Hospital discharge reports from national health care system on S-EHR;			Yes Satisfied by the R2D protocol specification

			#21: R2D import of (portion of) health data from all national health care systems on S-EHR; #37: R2D import of (portion of) Medical images and reports from national health care system on S-EHR; #74: R2D import of (portion of) Patient Summary from national health care system on S-EHR (with security); #98: Sharing of health data with qualified HCPs for emergency by means of S-EHR Cloud; #133: Automatic			

			download of health records from S-EHR Cloud to S-EHR			
		RDS	#110: Support of machine interpretable research protocol for publication.			No

Table 5 - Minimum Implementation of Technical Measures in user requirements

4.3. Constraints

In addition to these measures and extending the identified security goals, software vendors, operators and distributors as well as healthcare professionals and citizens must apply several organizational and procedural constraints in order to ensure citizens' rights and requirements regarding security and privacy.

These constraints are more restrictive than the ones applied by the GDPR to any software application. These constraints are:

- A S-EHR app provider cannot have access or give access, in any form, to the personal data processed by the S-EHR app of a Citizen.
- A S-EHR Cloud provider can have access or give access to the personal data of a Citizen only in encrypted format.
- A S-EHR Cloud provider must not have access or give access to any information that may allow to de-encrypt the personal data of a Citizen.
- Only the Citizen controls (i.e. determines) the exchange with any person or organisation of his/her personal data managed by the S-EHR app.
- The explicit and specific consent of the citizen is required for any exchange of sharing of personal data of the citizen with any organisation or person.
- Personal data may be stored by the S-EHR app or S-EHR Cloud on systems different from the mobile device where the S-EHR app is running and the system where S-EHR Cloud is running, only in encrypted format, only for the strict period that is necessary for the purpose of data transmission to other organisations or persons authorised by the Citizen.
- Personal Data must not be accessible or distributed beyond the intended and authorized use cases, actors and components, neither decrypted or encrypted.
- Personal Data must not leave organisational and system boundaries if not explicitly authorized, neither decrypted or encrypted, neither intended nor unintended, e.g. for further processing or backup purposes.
- Personal Data must not be processed by unauthorized or uncertified applications or components, e.g. a third party analytics application.
- Each application or component involved in the InteropEHRate use cases should be certified by a trustworthy and suited procedure and organization.
- The S-EHR application and the stored data must not be accessible by unauthorized entities, neither directly through a citizen's mobile device nor remotely through network access, e.g. in case of losses of mobile devices.
- The S-EHR application and stored data must not be usable or accessible by unauthenticated and unauthorized entities, e.g. unauthorized persons or processes.
- The user credentials for authentication and authorized use of the S-EHR application must not be known by anyone other than the owner or stored or distributed by any entity.
- A S-EHR application must not allow for an automatic authentication or automatic login.
- A S-EHR application must contain a privacy policy that explains how and why personal data is processed, applying data protection, privacy and security principles.

Each person or organization involved in the InteropEHRate use cases, software development and operation must apply these constraints in order to guarantee and enable a trustworthy operation and environment for the users, citizens and healthcare professionals.

5. CONFORMANCE LEVELS

The InteropEHRate Open Specification, groups the security requirements and constraints listed in the previous sections in different levels, called “conformance levels”.

A conformance level is a set of constraints to be satisfied by the S-EHR app or S-EHR Cloud (and by the hardware that it runs on) in order to be considered trustable by Citizens, healthcare organizations and research centres.

Each conformance level corresponds to a specific category of functionalities offered by the S-EHR and is intended to guarantee the citizens about risks that are specific to that category of functionalities.

They are called "levels" because the corresponding categories of functionalities are organised in a hierarchy (the category of a higher level includes the functionalities of the lower levels) and because for each category of functionalities different levels of increasing security are distinct.

Trusted organisations will check whether a S-EHR app or a S-EHR Cloud satisfies a specific conformance level and will authenticate the compliance of that specific application to that specific level. Indicating which are the organisations that will authenticate the compliance is out of the scope of this document. It may be decided by a consortium of organisations that adopt the InteropEHRate open specification and the citizens that trust them, or it may be legally regulated by a public authority that officially adopts the InteropEHRate open specification. The second option is preferable to better guarantee citizens’ rights.

For each kind of SW application, the InteropEHRate Open Specification distinguishes five functional categories corresponding to increasing **functional levels**:

1. Accessing & Storing = This level includes all security requirements related to storage of health data on S-EHR app and their backup on S-EHR Cloud (using the R2D Cloud protocol), and all the ones related to the download of health data from any EHR supporting the R2D protocol.
2. Receiving = This level includes all the security requirements and constraints of level 2 plus the ones related to the synchronous reception of health data on the S.EHR App thanks to the D2D protocol.
3. Explicit Sharing = This level includes all the security requirements and constraints of level 3 plus the ones of S-EHR app related to the synchronous sharing of health data using the D2D protocol.
4. Emergency Sharing = This level includes all the security requirements and constraints of level 4 plus the ones of S-EHR app and S-EHR Cloud related to the asynchronous sharing of health data for emergencies.
5. Research Sharing = This is the highest level, including all the previous security requirements and constraints and also the ones related to the asynchronous sharing of health data for research using the RDS protocol.

The functional level 1 is **mandatory** for any S-EHR app and S-EHR Cloud service, while all other functional levels are **optional**.

The following table (Table 6) shows the security requirements included in each functional level.

Level	Requirement	Application	Obligation
1	#10: Consent to S-EHR data management	S-EHR app	MANDATORY
	#70: Integrity of medical information	S-EHR app	MANDATORY
	#97: Activation of automatic backup of S-EHR content on selected S-EHR Cloud	S-EHR app + S-EHR Cloud	MANDATORY
	#133: Automatic download of health records from S-EHR Cloud to S-EHR	S-EHR app + S-EHR Cloud	RECOMMENDED
	#140: Auditing of citizens that gained access to their health data	S-EHR Cloud	DESIRABLE
	#69: Non repudiable data provenance tracking	S-EHR app	MANDATORY
	#135: Encryption of S-EHR content exchanged with S-EHR Cloud.	S-EHR app	MANDATORY
	#149: Citizen's consultation on S-EHR of S-EHR Cloud auditing data	S-EHR app + S-EHR Cloud	RECOMMENDED
2	#4: Auditing health data modification for Citizen on S-EHR	S-EHR app	RECOMMENDED
	#64: Consultation of auditing health data modification for Citizen on S-EHR	S-EHR app	RECOMMENDED
3	#13: D2D consent by the Citizen for temporary S-EHR access to Healthcare organization	S-EHR app	MANDATORY
	#17: D2D Identification and Authentication of the citizen from HCP	S-EHR app	MANDATORY
	#26: Enabling of Citizen identification from S-EHR (without CA)	S-EHR app	MANDATORY
	#76: Auditing health data sharing for Citizen on S-EHR	S-EHR app	RECOMMENDED
	#77: Consultation of auditing health data sharing for Citizen on S-EHR	S-EHR app	RECOMMENDED
	#78: Enabling of Citizen identification from S-EHR (with CA)	S-EHR app	DESIRABLE
4	#101: Auditing of HCPs that gained access for emergency reasons to Citizen's health data	S-EHR Cloud	MANDATORY
	#102: Auditing of changes to health data stored in the S-EHR Cloud	S-EHR Cloud	MANDATORY

	#105: Auditing of HCPs that gained access to the Medical Images	S-EHR Cloud	MANDATORY
	#134: Citizen's access to emergency token	S-EHR app	MANDATORY
	#137: Auditing of Organisations that gained access to health data for emergency reasons	S-EHR Cloud	RECOMMENDED
5	#86: Digitally signature by Reference Research Centre of Citizen's consent	S-EHR app	MANDATORY
	#87: Citizen's digital signature of consent to share health data for a given study	S-EHR app	RECOMMENDED
	#88: Citizen's digital revocation of consent to share health data for a given study	S-EHR app	MANDATORY
	#91: Automatic anonymization and sharing of citizen's health data for research.	S-EHR app	MANDATORY
	#107: Citizen's consent to be part of InteropEHRate Open Research Network	S-EHR app	MANDATORY
	#109: Citizen's withdrawing from research network	S-EHR app	RECOMMENDED
	#115: Support of description of pseudo-anonymization (yes/no) within data set definition	S-EHR app	MANDATORY
	#117: Support of specification of prospective period within dataset definition.	S-EHR app	MANDATORY
	#118: Support of specification of retrospective period within dataset definition.	S-EHR app	MANDATORY
	#120: Support of specification of Reference Centres within research protocol	S-EHR app	MANDATORY
	#122: Inclusion of human readable description of Coordinating and Local Research Centre within research protocol	S-EHR app	RECOMMENDED
	#123: Inclusion of human readable description of data retention period within the research protocol	S-EHR app	RECOMMENDED
	#124: Inclusion of human readable description of purpose of research within the research protocol	S-EHR app	RECOMMENDED
	#125: Inclusion of human readable description of usage restrictions of data within the research protocol	S-EHR app	RECOMMENDED
	#126: Citizen's consent to share health data for a research protocol	S-EHR app	MANDATORY

	#127: Citizens' selection of reference research centre	S-EHR app	DESIRABLE
	#128: Reception and storage of consent, digitally signed from research organisation, on Citizen's S-EHR	S-EHR app	MANDATORY
	#129: Signed consent refers to the research protocol accepted by the patient.	S-EHR app	MANDATORY
	#130: Pseudoidentity restricted to single research protocol.	S-EHR app	MANDATORY
	#132: Notification to Citizens of data sharing event for research	S-EHR app	RECOMMENDED

Table 6 - Security requirements included in each functional level

As shown by the table (Table 6) a security requirement may be mandatory, recommended or just desirable to have. Both desirable and recommended requirements are optional to implement, but a developer should assure that all recommended requirements are implemented before considering also the implementation of desirable ones.

A S-EHR app or a S-EHR Cloud implements a functional level if it implements at least all the mandatory requirements of that level. The functional level assigned to a S-EHR app or to a S-EHR Cloud service corresponds to the highest functional category that it implements.

An application that implements just the mandatory requirements of a level is considered (at that level) less secure than one that implements also the recommended requirements of the same level. An application that implements also the requirements that are desirable to have is considered to have the highest level of security.

More specifically, for every functional level three **security levels** are distinguished:

1. Minimum: the application satisfies all the mandatory security requirements of that functional level but not all recommended ones;

2. Standard: the application satisfies all mandatory and recommended security requirements of that functional level but not all the desirable ones;

3. Advanced: the application satisfies all security requirements of that functional level.

The security level of an application corresponds to the minimum implemented security level among the ones of all the implemented functional levels.

The couple composed by the security level followed by the functional level is the **conformance level** of the application.

E.g. a S-EHR app has security level 2 (Standard) and functional level 3 (Explicit Sharing) , or more simply has conformance level 2.3, if it implements all mandatory and recommended security requirements of the functional level 3, but does not implement all mandatory security requirements of functional level 4 (Emergency Sharing) and does not implement all the desirable security requirements of functional level 3

(although the application could implement all desirable requirements of level 1 and therefore be classified of Advanced security at functional level 1).

6. CONCLUSIONS AND NEXT STEPS

This document presents initial and general information on cyber risks and provides a first version of the InteropEHRate security conformance levels. The legal framework for data protection and data security has been discussed in detail. It was analysed which methods and solutions already exist and which criteria catalogues or guidelines have already been defined nationally / EU-wide. Since the topic of security is very extensive, the scope of our security requirements has been limited to the perspective of the project. Technical measures were assigned to the requirements and safety goals. Finally, the concept of security conformance levels is presented. This takes into account different dimensions that describe different aspects of conformity (range of functions, interoperability, security aspects).

The following content will be addressed in the next version of the document:

- Further refinement of security compliance levels taking into account the EU-wide strategy for the harmonization of security of networks and information systems (NISD).
- Definition of an assessment tool considering different perspectives (technical layer, organizational layer), stakeholders (developer, service provider, healthcare organization) and respectively different phases of the lifecycle of the S-EHR app / S-EHR Cloud (development, testing, operating).
- Definition of a security risk assessment process

The following list contains candidate additional technical measures regarding the security requirements, which are intended to be addressed in the next version of the document are other categories from ENISA's minimum security measures for Health sector [ENISA 2020 (2)] as well as the mapping to relevant standards such as HIPAA and ISO 27799 etc.

- Incident Report
- Logs correlation and analysis
- Detection
- Information system security incident response
- Human resource security
- Information system security indicators
- Information system security risk analysis
- Information system security accreditation
- Information system security policy
- Ecosystem relations
- IT security maintenance procedure
- System segregation

REFERENCES

- **[D2.2]** InteropEHRate Consortium, User Requirements for cross-border HR integration V2, 2020. www.interopehrate.eu/resources
- **[NAGARJUN 2018]** PMD Nagarjun and Shaik Shakeel Ahamad. "Review of Mobile Security Problems and Defensive Method". International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 12 (2018) pp. 10256-10259 https://www.ripublication.com/ijaer18/ijaerv13n12_20.pdf
- **[ALAZAB 2020]** M. Alazab, A. Shalaginov, A. Mesleh, A. Awajan. "Intelligent mobile malware detection using permission requests and API calls". *Future Gener. Comput. Syst. 2020*, *107*, 509–521.
- **[ENISA 2018]** ENISA, Privacy and data protection in mobile applications, 2018 https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications
- **[MDR 2017]** Regulation (EU) 2017/745 of the European Parliament and of the Council, "Medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC". (2017).
- **[EC 2016]** European Commission, "Guidelines on the Qualification and Classification of Stand Alone Software used in Healthcare within the Regulatory Framework on Medical Devices". MEDDEV 2.⅛. (2016) 20-21.
- **[EU 2012]** European Union, "Charter of Fundamental Rights of the European Union 2012/C 326/02, 26". (2012). Website: https://www.refworld.org/docid/3ae6b3b70.html.
- **[EDPS 2019]** European Data Protection Supervisor. "Charter Of Fundamental Rights". (2019). Website: https://edps.europa.eu/data-protection/our-work/subjects/charter-fundamental-rights_en.
- **[GDPR 2016]** Regulation (EU) 2016/679 of the European Parliament and of the Council. "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC". (2016).
- **[EDPB 2017 (1)]** Article 29 Data Protection Working Party, "Guidelines on Transparency under Regulation 2016/79". (2017), page 4.
- **[EDPB 2013]** Article 29 Data Protection Working Party, "Opinion on Purpose Limitation". (2013). Page 4
- **[EDPB 2017 (2)]** Article 29, Data Protection Working Party, "Guidelines on consent under Regulation 2016/679". (2017) 12-21.
- **[EDPB 2017 (3)]** Article 29, Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679". (2017).
- **[ENISA 2020 (1)]** ENISA. "Privacy and Data Protection in Mobile Applications A Study On The App Development Ecosystem And The Technical Implementation Of GDPR". (2020). Website:

https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications/at_download/fullReport.

- **[eIDAS 2014]** Regulation (EU) No 910/2014 of the European Parliament and of the Council, "Electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/9EC". (2014).
- **[ENISA 2016]** ENISA. "Security guidelines on the appropriate use of qualified electronic time stamps". (2016).
- **[ENISA 2020 (2)]** ENISA. "Minimum Security Measures for Operators of Essentials Services". (2020).
- **[RR 2012]** REGULATION (EU) No 531/2012 of the European Parliament and of the Council, "On roaming on public mobile communications networks within the Union". (2012).
- **[EC 2020]** European Commission. "*Roaming Charges, What Has The European Commission Done So Far?", - Shaping Europe's Digital Future - European Commission*. (2020). Website: https://ec.europa.eu/digital-single-market/en/roaming-charges-what-has-european-commission-done-so-far.
- **[RR 2017]** REGULATION (EU) 2017/920 of the European Parliament and of the Council, "Amending Regulation (EU) No 531/2012 as regards rules for wholesale roaming markets". (2017).
- **[NIST 2020]** Draft NIST Special Publication 800-57 Part 1 Revision 5, Recommendation for Key Management: Part 1 – General, May 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
- **[Sutton 2014]** Sinha, Amit, Michael Andrew William Sutton, and Srikanth Devarajan. "Systems and methods for mobile application security classification and enforcement." U.S. Patent No. 8,763,071. 24 Jun. 2014.
- **[Alenezi 2020]** M. Alenezi, A. Agrawal, R. Kumar, and R.A. Khan. "Evaluating Performance of Web Application Security through a Fuzzy based Hybrid Multi-Criteria Decision-Making Approach: Design Tactics Perspective". IEEE Access, 2020.
- **[Sönmez 2019]** F. Ö. Sönmez. "Security Qualitative Metrics for Open Web Application Security Project Compliance". Procedia Computer Science, 151 (2019): 998-1003.
- **[Bialas 2019]** A. Bialas. "Structurization of the common criteria vulnerability assessment process". International Conference on Dependability and Complex Systems (2019, July): 33-45. Springer, Cham.